LANDesk® Server Manager 8.6

Installation and Deployment Guide

LANDesk®

Contents

Overview

This guide walks you through the process of installing and deploying LANDesk® Server Manager, one of the most comprehensive network server management tools available.

Here's what you'll learn about in this overview:

- What's in this release
- Product basics (includes terms)
- Installation and deployment strategies
- Overview of installation and deployment

What's in this release

Server Manager is a device management product with a robust feature set. Devices include desktop, laptop, and server computers. Features new to this version include:

- **OS Deployment:** Provides PXE-based deployment to deploy OS images to devices on your network. This allows you to remotely image devices with empty hard drives or unusable OSes. Lightweight PXE representatives eliminate the need for a dedicated PXE server on each subnet.
- **Software licenses:** Implement complete, effective software asset management and license compliance policies.
- **Scheduled task view:** View or reschedule all agent deployment, vulnerability, software distribution, discovery, OSD, and user tasks from one location.
- **Enhanced OS support:** Manage all servers from a single console. Supports Windows 2000 and 2003, Red Hat Linux, SUSE Linux, HP-UX, and AIX. See Phase 1: System requirements for more information.
- **Intel* AMT support:** Supportfor Intel's Active Management Technology (AMT). Intel AMT provides the ability to remotely manage networked devices in any system state through out-of-band (OOB) communication. As long as the device is connected to a corporate network and has stand-by power, you can access inventory, view remote diagnostic information, and remotely reboot a system.
- **Scripting tool:** You can schedule and execute custom tasks on devices. You can create OS and file deployment scripts.
- **Task scheduler:** A single database schema with improved data integrity and scalability allows you to access a rich set of information about managed devices (including full integration with Management Suite). Part of this single schema is the task scheduler. You can now view all tasks (vulnerability, discovery, agent configuration, software distribution, scripts, and OS deployment) in a common window. From this window, you can reschedule, modify the schedule, or make the schedule to be recurring.

Some of the existing features include

- **Role-based administration:** Configure user access to tools and network devices based on user administrative role in your organization. With role-based administration, you assign scope to determine the devices a user can view and manage, and rights to determine the tasks they can perform.
- **Managed device discovery:** Discover devices on your network though a variety of methods. The product identifies servers running Windows or Linux, blade servers and

blade chassis, IPMI-enabled servers, Intel AMT-enabled servers, as well as other network devices. Schedule device discovery so you can constantly be aware of new devices. You can also generate reports on the unmanaged devices on your network. For more flexibility, you can now use a Device discovery task to rediscover managed devices. This is useful if you've reset your database.

- **Enhanced security:** A certificate-based security model allows devices to only communicate with authorized core servers and consoles.
- **Health monitoring:** Monitor important device functions and resources to alert you to problems as soon as the product becomes aware of them. Depending on the device's hardware, resources and functions, this product can monitor items such as running services, power supplies, temperatures, voltages, and hard disk space usage.
- **Software distribution:** Automate the process of installing software applications or distributing files to devices.
- **On-demand remote control:** The highly stable (Ring-3) on-demand remote control model only loads the remote control agent on servers for the duration of an authorized remote control session. Detailed remote control logs are stored in the database. Log information includes who initiated the remote control session and the remote control tasks (such as file transfers) they performed on the device. Also, remote control sessions now pass third mouse button/wheel movement to devices.
- **Reports:** Predefined service reports are available for planning and strategic analysis.
- **Software summary:** View details about a device by double-clicking it and clicking **Summary** in the left navigation pane.
- **Scheduled task support:** Provide multiple logins for the scheduler service to authenticate with when running tasks on devices that don't have agents. This is especially useful for managing devices in multiple Windows domains.
- **Vulnerability scanner:** Create user-defined vulnerability scans so you can detect problems before a patch is available. You can scan for vulnerabilities provided by major vendors, download patches, and remediate all from your workstation.
- **Dashboard**: Provides at-a-glance health of all the managed devices on your network.

Product basics

Server Manager supports Windows* 2000/2003 servers, Red Hat Enterprise Linux v3 servers, SUSE Linux 9 servers, HP-UX and AIX servers, and it provides a common interface for managing the devices of these network operating systems. It can co-exist with other LANDesk products, too, such as LANDesk® Management Suite.

How does the product fit into my network?

This product uses the infrastructure of your existing network to establish connections with the devices it manages. The job of managing your existing devices is greatly simplified, whether you manage a small network or a large enterprise environment.

How can Server Manager and Management Suite co-exist in my environment?

Server Manager and Management Suite can co-exist in your environment providing full management of desktops, laptops, and servers. You can install both applications on the same core server, or on separate servers.

Server Manager supports the installation of a single core to a single database. Therefore, if you install Server Manager and Management Suite on the same device,

both products must use the same database. If you install Server Manager and Management Suite on different devices, the applications must point to different databases (or "tablespaces" in Oracle).

Upgrading from Management Suite 8.0/8.1 with System Manager

Upgrading LANDesk Server Manager 8.0/8.1 installed requires an agent upgrade to the Server Manager 8.6 agent. This is done by deploying the Server Manager 8.6 agent to those machines, either by push or pull. For Client Manager 6.3, nodes must be manually removed through **Control Panel | Add/Remove Programs**.

To upgrade from Management Suite 8.0/8.1 with System Manager or Management Suite 8.5/Server Manager to Server Manager, follow those steps:

1. Add Server Manager to the core by completing the steps shown in Phase 3: Installing the core server.

2. From the Management Suite console, deploy the client agent to client nodes so that they may be seen from the Server Manager console. For information on how to configure agents and push agents from the Management Suite core, see the **Configuring device agents** chapter in the *Management Suite User's Guide*.

Upgrading from Server Manager 8.5

Upgrading from version 8.5 is easy. When you install this version, the installation notes that a previous version is installed, and asks if you want to use a previous database. Select **Yes** to install using the previous database and retain data from your previous product version.

Product terms

- **Core server:** The center of a management domain. All the product's key files and services are on the core server. A management domain has only one core server.
- **Console:** The browser-based console that is the main product interface.
- **Core database:** The product requires one database for each core server.
- **Managed devices:** Devices in your network that have LANDesk agents installed. A core server can manage thousands of devices. Larger environments require multiple core servers.

Core server system requirements

As you consider which server you'll set up as your core server, review these system requirements and confirm that your server meets or exceeds them:

- Windows 2000 Server or Advanced Server with SP 4 or Windows Server 2003 Standard or Enterprise edition (SP1 is recommended but not required)
- Microsoft Data Access Components (MDAC) 2.8 or higher
- Microsoft .NET Framework 1.1
- Internet Information Services (IIS)
- IIS support for ASP.NET v1.1 scripting

- Internet Explorer 6.0 SP1 or higher
- Microsoft NT File System (NTFS)
- The Windows server you use for your core server must be a standalone server, not as a primary domain controller (PDC), backup domain controller (BDC), or Active Directory controller.
- SNMP must be installed, and SNMP and SNMP trap services must be started
- 200 MB of space available on the system drive, and 900 MB of space available on at least one drive
- Administrator privileges
- LANDesk client is either the correct version or not installed

---

A dedicated core server is strongly recommended
Because of the traffic that passes through the core server to manage your domain, we strongly recommend that each core server or database server is dedicated to hosting the product.

If you install other products on the same server, you may experience short- and long-term resource issues.

Don't install the core server components on a primary domain controller, backup domain controller, or active directory controller.

Installation and deployment strategies

Installing and deploying a system-wide application to a heterogeneous network requires a deliberate methodology and significant planning *before* you run the setup program. This guide includes strategies for setting up the product. Before deploying it, you need to briefly characterize your management needs.

Deployment strategy considerations

Deployment is the process of expanding your management capabilities to servers that you want to include in the domain. Deployment is simplified when you load agents and services on devices so that you can manage them from a central location. In this guide, deployment is discussed in "phases."

The phased deployment strategy offers you a structured approach to enabling management on devices. This approach is based on two simple principles:

- First, deploy those product components that have the least impact on your existing network and progress to those components that have the most impact.
- Second, deploy the product in well-planned stages, rather than deploying all services at once, which may complicate any required troubleshooting.

This guide is organized sequentially to help you deploy the product. See the first chapter, Phase 1: Designing your management domain later in this guide. You should then continue sequentially through each phase.

Overview of installation and deployment

This guide groups installation and deployment tasks into the following phases. Each phase has a corresponding section in this guide that walks you through that part of the installation. The Getting Started chapter is designed to help you start using Server Manager quickly by configuring services, running the console, discovering devices, moving the devices into the Managed list, and configuring the managed devices for actions. It is designed to be succinct, assuming that you will consult the rest of the book for detail. Some of the procedures in this guide are repeated in the Getting Started chapter.

Phase 1 summary

During phase 1 of the installation, you design your management domain by completing these tasks:

- Gather network information
- Confirm that your network meets system requirements

For details, refer to Phase 1: Designing your management domain later in this guide.

Phase 2 summary

During phase 2 of the installation, you prepare your databases by completing these tasks:

- Install and configure your databases
- Conduct basic database maintenance

For details, refer to Phase 2: Preparing your databases later in this guide.

Phase 3 summary

During phase 3, you install the product by completing these tasks:

- Install the core server
- Maintain the database

For details, refer to Phase 3: Installing the core and console later in this guide.

Phase 4 summary

During phase 4 of the installation, you discover devices on your network and deploy the product agents. You can push the agents from the console or pull them from the server share.

For details, refer to Phase 4: Deploying the agents to devices later in this guide.

Getting Started

Getting started

Overview

Welcome to LANDesk® Server Manager, a stand-alone device management application that maximizes your valuable time by letting you quickly and efficiently manage your devices. Server Manager lets you view your devices in a central location, group them for actions (such as power cycling, vulnerability assessments, or configuring alerts), remotely troubleshoot any problems, and keep your devices updated with the latest patches.

This guide's purpose is to help you start using Server Manager quickly by configuring services, running the console, discovering devices, moving the devices into the Managed list, and configuring the managed devices for actions.

Server Manager is a Web application, allowing you to access it using your browser so you can manage your servers from a remote workstation. It behaves like many of the Web applications which you are accustomed to, but it also contains several advanced Windows-type controls to enhance your usability experience. For example, hover the mouse pointer over a control then double-click it or right-click it (just as you would in a Windows application). For example, in the **My devices** list, you can double-click a device name to access its specific information, or right-click to see available actions.

The steps below guide you through getting Server Manager up and running, discovering devices on your network, selecting the servers to move to your **My devices** list, deploying agents, and then targeting those devices for various tasks.

Running the installation program

During the install, on the Autorun page, select LANDesk Server Manager.

After you have installed Server Manager, you are ready to start using it. The sections below tell you how to complete several required tasks: running the core activation utility, configuring services, discovering computers, specifying which devices to

actively manage by moving the devices the **My devices** list, grouping devices, adding users, and deploying agents.

Activating the core server

Use the Core Server Activation utility to:

- Activate a new Server Manager core server for the first time
- Update an existing Server Manager core server or switch from a trial-use license to a full-use license

Each core server must have a unique authorization certificate.

With your core server connected to the Internet,

1. Click **Start | All Programs | LANDesk | Core Server Activation**.
2. Type in the unique user name and password provided by LANDesk when you purchased your licenses.
3. Click **Activate**.

The core communicates with the LANDesk Software licensing server via HTTP. If you use a proxy server, click the utility's **Proxy** tab and enter your proxy information. If your core has an Internet connection, communication with the license server is automatic and won't require any intervention by you.

Periodically, the core server generates node count verification information in the "\Program Files\LANDesk\Authorization Files\LANDesk.usage" file. This file gets sent periodically to the LANDesk Software licensing server. This file is in XML format and is digitally signed and encrypted. Any changes made manually to this file will invalidate the contents and the next usage report to the LANDesk Software licensing server.

- The Core Server Activation utility won't automatically launch a dial-up Internet connection, but if you launch the dial-up connection manually and run the activation utility, the utility can use the dial-up connection to report usage data.
- You can also activate the core server by e-mail. Send the file with the .SAVE extension located under Program Files\LANDesk\Authorization to licensing@landesk.com. LANDesk customer support will reply to the e-mail with a file and instructions on copying the file to the core server to complete the activation process.

Adding users

Server Manager users are users who can log in to the console and perform specific tasks for specific devices on the network. When you install the product, two user accounts are automatically created (see below). If you want to add more users, you can do so manually.

Users are not actually created in the console. Instead, users appear in the Users group (click **Users** in the left navigation pane) after they have been added to the LANDesk Management Suite group in the Windows NT users environment on the core server. The Users group shows all of the users currently residing in the LANDesk Management Suite group on the core server.

There are two default users in the Users group:

Default Template User—This user contains a template of user properties (rights and scope) that is used to configure new users when they are added to the Management Suite group. In other words, when you add a user to that group in the Windows NT environment, the user inherits the rights and scope currently defined in the Default Template User properties. If the Default Template User has all rights selected and the Default All Machines Scope selected, any new user placed in the LANDesk Management Suite group will be added to the Users group with rights to all of the product tools and access to all devices.

You can change the property settings for the Default Template User by selecting it and clicking **Edit**. For example, if you want to add a large number of users at once, but do not want them to have access to all of the tools or devices, change the settings for the Default Template User first, then add the users to the LANDesk Management Suite group (see steps below).

The Default Template User cannot be removed.

Default Administrator—This is the administrative user who was logged in to the server when Server Manager was installed.

When you add a user to the LANDesk Management Suite group in Windows NT, the user is automatically read into the Users group in the **Users** window, inheriting the same rights and scope as the current Default Template User. The user's name, scope, and rights are displayed. Additionally, new user subgroups, named by the user's unique login ID, are created in the User Devices, User Queries, User Reports, and User Scripts groups (note that ONLY an Administrator can view User groups).

Conversely, if you remove a user from the LANDesk Management Suite group, the user no longer appears in the **Users** list. The user's account still exists on the core server and can be added back to LANDesk Management Suite group at any time. Also, the user's subgroups under User Devices, User Queries, User Reports, and User Scripts are preserved so that you can restore the user without losing their data, and so that you can copy data to other users.

Refresh the frame by pressing F5.

To add a user or domain group to the LANDesk Management Suite group

1. Navigate to the server's **Administrative Tools** | **Computer Management** | **Local Users and Groups** | **Groups** utility.
2. Right-click the LANDesk Management Suite group, and then click **Add to group**.
3. Click **Add**, then type or select a user (or users) from the list.
4. Click **Add**, and then **OK**.

Note: You can also add a user to the LANDesk Management Suite group by right-clicking the user account in the **Users** list, clicking **Properties** | **Member Of**, and then clicking **Add** to select the group and add the user.

If user accounts do not already exist on the server, you must first create them on the server.

To create a new user account

1. Navigate to the server's Administrative **Tools** | **Computer Management** | **Local Users and Group** | **Users** utility.
2. Right-click **Users**, and then click **New User**.
3. In the **New User** dialog, enter a name and password.
4. Specify password settings.
5. Click **Create**. The **New User** dialog remains open so that you can create additional users.
6. Click **Close** to exit the dialog.

Add the user to the LANDesk Management Suite group to have them appear in the **Users** group in the console.

Configuring services and credentials

Before you can manage devices on your network, you must provide Server Manager with the necessary credentials. Use the Configure Services utility on the core (SVCCFG.EXE) to specify the required operating system, Intel* AMT, and IPMI BMC credentials. You can also specify additional settings, such as inventory defaults, PXE holding queue settings, and LANDesk database settings.

Use Configure Services to configure:

- The database name, username, and password. (Set at installation time.)
- Credentials for scheduling jobs to the managed devices. (You can enter more than one set of administrator credentials.)
- Credentials for configuring IPMI BMCs. (You can enter only one set of BMC credentials.)
- Credentials for configuring Intel AMT-enabled devices. (You can enter only one set of Intel AMT credentials.)
- Server software scan interval, maintenance, days to keep inventory scans, and login history length.
- Duplicate device ID handling.
- Scheduler configuration, including scheduled job and query evaluation intervals.
- Custom job configuration, including remote execute timeout.

1. At the core server, click **Start | All Programs | LANDesk | LANDesk Configure Services**.
2. Click the **Scheduler** tab.
3. Click the **Change Login** button.
4. Enter the credentials you want the service to use on the managed devices, typically a domain administrator account.
5. Click **Add**. Add additional credentials as necessary, if the managed devices do not all have the same administrator user name accounts enabled.
6. Click **Apply**.
7. If you have IPMI-enabled servers in your environment, click the **BMC Password** tab. Type a password in the **Password** text box, retype the password in the **Confirm password** text box, then click **OK**. (All managed IPMI servers must share the same BMC user name and password.)
8. Set any other settings as desired, such as software scan intervals.
9. Click **OK** to save the changes.

Click **Help** on each Configure Services tab for more information.

Running the console

Server Manager includes a full range of tools that let you view, configure, manage, and protect the devices on your network. The convenience of the console is that you can perform all of its functions from a remote location, such as your workstation - freeing you from the need to take additional trips to the server room or to go to each managed device individually to perform routine maintenance or troubleshoot problems.

Launch the console one of three ways:

- On the core server, click **Start | All Programs | LANDesk | Server Manager**.
- In a browser at a remote workstation, type the URL *http://coreserver/LDSM*.
- In the dashboard, click **LDSM console**.

Discovering devices

Use the Discovery Configuration dialog box to customize a scan to find unmanaged devices on your network. Use this dialog to isolate subnets or types of devices to reduce network traffic or the time required to complete the discovery task.

1. In the left navigation pane, click **Device discovery**.
2. On the **Discovery configurations** tab, click **New**.
3. Fill in the fields described below. When you are finished, click **OK**.

The text below describes the parts of the **Discovery configuration** dialog box.

- **Configuration name:** Type a name for this configuration.
- **Network scan (recommended):** Looks for devices by sending ICMP packets to IP addresses in the range you specify. By default, this option uses NetBIOS to try and gather information about the device.
    - The network scan option also has an **IP fingerprinting** option, where device discovery tries to discover the OS type through TCP packet responses. The IP fingerprinting option returns the most thorough information available, but it can take longer to complete.
- **LANDesk CBA:** Looks for the standard LANDesk agent (formerly known as the common base agent, CBA, in Management Suite) on devices.
- **IPMI:** Looks for IPMI-enabled servers. Intelligent Platform Management Interface (IPMI) is a specification developed by Intel,* H-P,* NEC,* and Dell* to define the message and system interface for management-enabled hardware. IPMI contains monitoring and recovery features that let you access many features regardless of whether the system is turned on or not, or what state the OS may be in.
- **Chassis:** Looks for blade server chassis using the IBM/Intel architecture. The blade servers themselves are discovered using a standard network scan.
- **Intel* AMT:** Looks for devices with Intel* Active Management Technology-enabled devices installed. AMT is a platform-resident hardware and firmware solution that uses out-of-band communication to allow remote management regardless of the state of the operating system or platform power.

- **Starting IP:** Enter the starting IP address for the range of addresses you want to scan.
- **Ending IP:** Enter the ending IP address for the range of addresses you want to scan.
- **Subnet mask:** Enter the subnet mask for the IP address range you're scanning.
- **Add:** Adds your IP address range to the work queue at the bottom of the dialog.
- **Clear:** Removes the IP addresses and subnet mask from the text boxes.
- **Remove/Remove All:** Clears IP address ranges from the queue.

Now that you have configured a discovery, you can discover the devices connected to your network.

Scheduling and running the discovery

Use the **Schedule** button on the **Discover devices** tab to display the **Schedule discovery** dialog. Use this dialog to schedule when a discovery or a deployment will run. You can schedule a discovery or client configuration to run immediately, at some point in the future, make it a recurring schedule, or run it just once and never worry about doing it again.

Once you schedule a discovery or deployment, see the **Discovery tasks** tab for discovery status. Scheduling a recurring discovery assists you by automatically discovering new devices that come up on the network

The **Schedule discovery** dialog has these options.

- **Leave unscheduled**: Leaves the task unscheduled but keeps it in the **Discovery configurations** list for future use.
- **Start now**: Runs the task as soon as possible. It may take up to a minute for the task to start.
- **Start later**: Starts the task at the time you specify. If you click this option, you must enter the following:
    - **Time**: The time you want the task to start
    - **Date**: The date you want the task to start. Depending on your locale, the date order will be day-month-year or month-day-year.
    - **Repeat every**: If you want the task to repeat, select whether you want it to repeat **Daily**, **Weekly**, or **Monthly**. If you pick Monthly and the date doesn't exist in all months (for example, 31), the task will only run in months that have that date.

To schedule a discovery

1. In the left navigation pane, click **Discovered devices**.
2. On the **Discovery configurations** tab, select the configuration you want and click **Schedule**. Configure the discovery schedule and click **Save**.
3. Monitor the discovery progress in the **Discovery tasks** tab. Click **Refresh** to update the status.

4. When the discovery completes, click **Unmanaged** to view all discovered devices in the upper **Discovered devices** pane (the pane does not refresh automatically).

Viewing discovered devices

Discovered devices are categorized by device type in the **Discovered devices** pane. The **Computers** folder is displayed by default. Click the folders in the left pane to view devices in different categories. Click **Unmanaged** to view all devices returned by the discovery.

- Intel AMT-enabled devices appear in the **Intel AMT** folder.
- Blade chassis servers appear in the **Chassis** folder.
- Standard enterprise devices appear in the **Computers** folder.
- Routers and other devices appear in the **Infrastructure** folder.
- IPMI-enabled servers appear in the **IPMI** folder.
- Non-categorized devices appear in the **Other** folder.
- Printers appear in the **Printers** folder.

Note: Some Linux servers appear with the generic "Unix" as the operating system name (or even sometimes show as Other). When the standard LANDesk agent is deployed, these servers will update their OS name entry in the **My devices** list and display a full inventory.

To view discovered servers

1. In the **Device discovery** page, in the left pane, click **Computers** or another type of device you want to view. The results are displayed in the right pane.
2. To filter the results, click the Filter icon, type at least a portion of what you are searching for, and click **Find**.

Assigning names

When doing a network scan discovery, some servers return with blank node name (or host name). This occurs most frequently with servers running Linux. You must assign a name to the device before you can use Manage to move it to the My devices list.

1. In the **Device discovery** page, click the device with a blank name. (You must click the blank area in the node name column.)
2. Click **Assign name** on the toolbar.
3. Type in the name and click **OK.**

When you install a product agent on a device, it automatically scans the host name and updates the core database with the correct information.

Moving devices to the My devices list

Once discovered, you must manually target the devices you wish to manage and move them to the **My devices** list. Moving the device does not install any software

to the device. It only makes the device available for querying, grouping, and sorting in the **My devices** list.

1. In the **Discovered devices** view, click the device you want to move to the **My devices** list. You can select multiple devices by pressing SHIFT+click or CTRL+ click.
2. Click the **Target** button. If it is not visible, click or<< on the toolbar. The button is on the far right. Or, right-click the selected servers and click **Target**.
3. Click the **Manage** tab.
4. Select to move selected devices to the management database or select to move targeted devices.
5. Click **Move**.

   Clicking **Move** moves the servers to the **My devices** list and places the device's information to the database. Once the information is in the database, you can run limited queries and reports on it (such as by device name, IP address or OS).

Note: If you choose to install the product agents manually by building them into a server image or by pulling the agentry from the core server's LDLogon share, the devices automatically appear in the **My devices** list. You will not have to discover the devices and explicitly move them to the **My devices** list.

Grouping devices for actions

You may want to organize your devices into groups, such as by geographic location or function, so you can perform actions on them more quickly. For example, you may want to see the processor speeds of all the servers in a specific location.

1. In the **My devices** list, click **Private groups** or **Public groups**, then click **Add group**.
2. Type a name for the group in the **Group name** box.
3. Click the type of group you want to create.

   - **Static**—Devices that have been added to the group. They remain in the group until they are removed or until you no longer manage them.
   - **Dynamic**—Devices that meet one or more criteria as defined by a query. For example, a group may contain all servers that are currently in a Warning state. They remain in the group as long as they match the criteria defined for the group.

   To associate a query with a group, create the group, then click **My devices**, click **Public groups** or **Private groups**, click the group, then under Properties, click **Create a filter based on an existing query**. Select the query, then click **Create filter**.

4. When you are finished, click **OK**.
5. To add devices to a static group, click devices in the right pane of the **My devices** list, click **Move/Copy**, select the group, and click **OK**.

Devices are automatically added to dynamic groups when they meet the group query criteria.

Configuring devices for management

Before you can fully manage devices with the console and receive health alerts, you need to install Server Manager management agents on them. You can choose to install the default agent configuration (which installs all LANDesk agents) or customize your own agent configuration to install on your devices. (The agent configuration must include the monitoring agent to receive health alerts.)

To install management agents:

- Target devices in the **My devices** list, then schedule an agent configuration task to remotely install agents on the devices.
- Map to the core's LDlogon share (//coreserver/ldlogon) and run SERVERCONFIG.EXE.
- Create a self-extracting device installation package. Run this package locally on the device to install the agents. This must be done while logged in with administrative privileges.

To pull the agent from the LDlogon share (only works on Windows devices):

1. At the system you want to configure, click **Start > Run**, then type *\\coreserver\ldlogon\ServerConfig.exe*.
2. Select the components you want to configure the system with, then click **Install.**
3. Follow the on-screen instructions.

The system now has the selected Server Manager agents installed. No reboot is required. The server is automatically added to the **My devices** list.

To push the agent:

1. Target devices in the **My devices** list (as explained above in Moving devices to the My devices list)
2. In the left navigation pane, click **Agent configuration**, right-click the configuration you want to push, and click **Schedule task**.
3. In the left pane, click **Target devices**, and click the **Add target list** button.
4. Click **Schedule task**, click **Start now** to start the task immediately or **Start later** and set the task's start date and time, and click **Save**.

You can view the status of the task in the **Configuration tasks** tab.

Running the dashboard

The dashboard is a simple, high-level, uncluttered view of your devices. It represents each device with an icon whose color represents the device's current health. The dashboard also provides quick access to key troubleshooting tools.

To launch the dashboard:

- On the core server, click **Start | All Programs | LANDesk | Server Manager Dashboard**.
- In a browser at a remote workstation, type the URL *http://coreserver/LDSM/db_frameset.asp*.
- In the console, click **Dashboard**.

*Other brands and names may be claimed as the property of others.

Phase 1: Designing your management domain

In phase 1, you gather information about your network infrastructure and make decisions that help you customize your management domain.

In this phase you'll learn about:

- Gathering network information
- Selecting your core server
- Selecting a database
- Planning your security and organization model
- System requirements

Gathering network information

Identify and collect all critical information about your network as it relates to Server Manager. Specifically, you need to:

- Determine the number of sites
- Estimate the number of devices at each location
- Select your core server
- Plan placement of program files
- Select a database
- Determine the number of domains
- Understand the functionality available by OS

Determining number of sites

First, identify all site locations where you want to deploy this product. You'll use this information to determine the size and reach of each management domain, as well as the placement of core servers and database servers.

To get this information, refer to your corporate WAN or LAN topology charts and server configuration charts.

Estimating number of devices at each location

You need to identify how many devices per site will be managed by this product and gather preliminary information about those devices. You'll use this information to determine domain size, select a database, and compare with the product system requirements.

The more information you can gather about the type of devices you'll manage, the better you can plan. Even rough estimates can help.

Determining device configurations

Gather configuration information on each device that you plan to manage. You'll use this information later in the domain design process to help determine if the servers you've selected meet the system requirements for a core server and database server. Identify this information for each device that will be managed:

- Type of processor
- Network operating system version, plus applied service packs or patches
- Approximate available disk space
- Hard disk type (for example, ultra-wide SCSI, disk arrays, and so on)
- RAM

Selecting your core server

The core server is the center of a management domain. All the key files and services are contained on the core server. A management domain can have only one core server.

You can run the administrator console from a browser on a remote workstation, where you conduct management activities such as taking remote control of a device, querying the core database, or distributing a software package.

Make sure that the server(s) you select for your core server meet the system requirements. Refer to system requirements later in this phase.

Planning placement of program files

During installation, you can specify where you want to install the program files. Accept the default destination directories unless you have compelling reasons to change them. If you choose to modify the destination directory, the destination directory path cannot contain double-byte characters.

The default destination directory for core server files is:

```
C:\Program Files\LANDesk\ManagementSuite
```

Selecting a database

LANDesk support several types of databases. MSDE is the default, but is not recommended for enterprise-scale installations. For information on databases and LANDesk, please go to http://www.landesk.com/support/downloads/Resource.aspx?pvid=31&rtid=9.

Each MSDE database has a 2 GB database size limit. The number of servers this database supports depends on your network's inventory scan file size. In larger environments, you should use the supported Microsoft SQL or Oracle* 8i or 9i databases to keep the product performing optimally. In these larger environments, the MSDE database won't perform as well as a true enterprise-level database.

You'll likely see performance issues with MSDE when the database has more than five concurrent things to do. If you want to use MSDE, consider how often you might have more than five people accessing the database at exactly the same time. If it's likely more than five people will be accessing the database, what will those people be

doing? For example, if they're all running software-related queries against the core database, use SQL Server or Oracle, since software-related queries can take a while to complete because of the amount of data involved. If they're all querying the core database for a set of servers with a certain hard drive size, you can probably stay with MSDE, since that type of query usually takes less than a second to complete.

If you want or need to use your own database, you can select either:

- Microsoft SQL Server 2000 SP 4
- Oracle* 8i (8.1.7)
- Oracle* 9i (9.2.0.4)

For detailed information about databases, refer to Phase 2: Preparing your databases later in this guide.

Planning your security and organization model

Devices authenticate to their authorized core server before communicating with the core, and role-based administration allows product administrators to control the rights console users have and which devices they can work with (scope).

You should decide how you want to handle security before deploying the product, because changing security requires you to redeploy client agents or security certificates.

Planning your core server structure

This product uses a certificate-based authentication system. During the core installation, Setup creates a certificate for that core. Clients look for that certificate when communicating with the core, and clients won't communicate with a core for which they do not have a certificate.

Devices will only communicate with core servers that the device has a matching trusted certificate file for. Each core server has its own certificate and private keys, and by default, the client agents you deploy from each core server will only talk to the core server from which the software is deployed.

Planning a scope

Role-based administration is a powerful feature for feature security management. Access the role-based administration tools in the console by clicking **Users** in the left pane. You must be logged in with administrative rights.

Role-based administration provides advanced device management capability by letting you add users to your system and assign those users rights and scopes. Rights determine the tools and features a user can see and use (see "Understanding rights" in the *User's Guide*). Scope determines the range of devices a user can see and manage (see "Creating scopes" in the *User's Guide*).

You can create roles based on users' responsibilities, the management tasks you want them to perform, and the devices you want them to see, access, and manage. Access to devices can be restricted to a geographic location such as a country, region, state, city, or to a specific group or type of server.

For example, you can have one or more users in charge of software distribution, another user responsible for remote control operations, another user who runs reports, and so on. To implement and enforce this type of role-based administration across your network, simply set up current users, or create and add new users as product users, and then assign the necessary rights (to product features) and scope (to managed devices).

The core server uses scopes to limit the devices that console users can see. Multiple scopes can be assigned to a user, and one scope can be used by multiple users. You can base scopes on one of these methods:

- **(Default) All Machines Scope:** Users can see all devices.
- **(Default) No Machines Scope:** Users are unable to see any devices.
- **Based on a Query:** Users can see the devices that fit the selected criteria of a specific query assigned to them by the administrator.
- **Based on a Group:** Users can see the devices that meet the group criteria.

For more information on scopes, see the *User's Guide*.

Understanding certificates

The certificate-based authentication model has been simplified. Client agents still authenticate to authorized core servers, preventing unauthorized cores from accessing devices. However, this product doesn't require a separate certificate authority to manage certificates for the core and each device. Instead, each core server has a unique certificate and private key that Setup creates when you first install the core server.

System requirements

Make sure that you meet the following system requirements before you install.

Core and database servers

Make sure that all of your core and database servers meet the requirements in the overview.

- Windows 2000 Server or Advanced Server with SP 4 or Windows Server 2003 Standard or Enterprise edition
- Microsoft Data Access Components (MDAC) 2.8 or higher
- Microsoft .NET Framework 1.1
- Internet Information Services (IIS)
- IIS support for ASP.NET v1.1 scripting
- Internet Explorer 6.0 SP1 or higher
- Microsoft NT File System (NTFS)
- The Windows server you use for your core server must be installed as a standalone server, not as a primary domain controller (PDC), backup domain controller (BDC), or Active Directory controller.
- SNMP must be installed, and SNMP and SNMP trap services must be started
- 200 MB of space available on the system drive, and 900 MB of space available on at least one drive

- Administrator privileges
- LANDesk client is either the correct version or not installed

---

Core server requirements
The Windows pagefile should be at least 12 + *N* (where *N* is the number of megabytes of RAM on the core server). Otherwise, product applications may generate memory errors.

All product services hosted on one server

For smaller management domains, you can install the core server and the core database on one server. For these networks, you may want to consider using the default Microsoft MSDE database, which is generally easier to maintain.

Limitation considerations

Your server should at least meet these system requirements before you install:

- Pentium 4 processor
- 4 GB of free disk space on 10K RPM or faster drives
- 768 MB+ of RAM

Managed server computers

This product supports these server operating systems (not all operating systems are supported equally):

- Microsoft Windows 2000 Server (with SP4)
- Microsoft Windows 2000 Advanced Server (with SP4)
- Microsoft Windows 2000 Professional (with SP4)
- Microsoft Windows 2003 Server Standard Edition (with SP1)
- Microsoft Windows 2003 Server Standard x64 Edition (with SP1)
- Microsoft Windows 2003 Server Enterprise Edition (with SP1)
- Microsoft Windows 2003 Server Enterprise x64 Edition (with SP1)
- Microsoft Windows XP Professional (with SP2)
- Windows Small Business Server 2000 (with SP4)
- Windows Small Business Server 2003 (with SP1)
- Red Hat Enterprise Linux v3 (ES)
- Red Hat Enterprise Linux v3 (ES) EM64t
- Red Hat Enterprise Linux v3 WS
- Red Hat Enterprise Linux v3 WS EM64t
- Red Hat Enterprise Linux v3 (AS)
- Red Hat Enterprise Linux v3 (AS) EM64t
- SUSE* Linux Server 9
- SUSE Linux Enterprise Server 9 EM64t
- HP-UX 11.1
- Unix AIX

Linux managed server computers

Below is a list of the prerequisites for enabling Linux devices for management.

Firewall

In order to initially install the LANDesk management agent and configure a Linux server to communicate with the core (using the "Push" method), SSH connections must be allowed to pass through the Linux server's local firewall:

22 - TCP only

In order for the agents to be able to communicate with the Core server(s) (for inventory scans, software distribution, vulnerability updates, and so forth), the Linux server's local firewall must be configured to allow communication on the following ports:

9593 - TCP only

9594 - TCP only

9595 - both TCP and UDP

In order to communicate with the LANDesk Server Manager agent, the Linux server's local firewall must be configured to allow communication on the following ports:

6780 - TCP only

Required RPMs (version # or later)

It is recommended that you store all LANDesk management RPMs in the ...\ManagementSuite\ldlogon\RPMS directory. You can browse to this directory through http://*core name*/RPMS.

REDHAT_ENTERPRISE

perl

RPM Version:5.8.0-88.4

Binary Version:5.8.0

python

RPM Version:2.2.3-5

Binary Version:2.2.3

pygtk2

RPM Version:1.99.16-8

Binary Version:

sudo

RPM Version:1.6.7p5-1

Binary Version:1.6.7.p5

bash

RPM Version:2.05b-29

Binary Version:2.05b.0(1)-release

xinetd

RPM Version:2.3.12-2.3E

Binary Version:2.3.12

mozilla

RPM Version:

Binary Version:1.5

openssl

RPM Version:0.9.7a-22.1

Binary Version:0.9.7a

perl-CGI

RPM Version:2.81-88.4

Binary Version:2.81-88.4

perl-Filter

RPM Version:1.29-3

Binary Version:1.06

sysstat

RPM Version:4.0.7-4

Binary Version:4.0.7

SUSE LINUX

(SuSE 64)

bash

RPM Version: 2.05b-305.6

mozilla

RPM Version: 1.6-74.14

mysql

RPM Version: 4.0.18-32.9

mysql-server

RPM Version:NA [provided by mysql]

net-snmp

RPM Version: 5.1-80.9

openssl

RPM Version: 0.9.7d-15.13

perl

RPM Version: 5.8.3-32.1

perl-CGI

RPM Version: NA [provided by perl]

perl-DBD

RPM Version:mysql-2.9003-22.1 [note: case change]

perl-DBI

RPM Version: 1.41-28.1

perl-Filter

RPM Version: NA [provided by perl]

python-gtk

RPM Version: 2.0.0-215.1 [note: package name change]

python

RPM Version: 2.3.3-88.1

sudo

RPM Version: 1.6.7p5-117.1

sysstat

RPM Version: 5.0.1-35.1

xinetd

RPM Version: 2.3.13-39.3

lm_sensors

RPM Version: NA (note: this has been incorporated into the kernel for the 2.6 version)

Product port usage

Introduction

When using this product in an environment that includes firewalls (or routers that filter traffic), you may need to adjust firewall or router configurations to allow the product to operate. This section describes the ports used by the various product components. The information here focuses on information you need to configure routers and firewalls, leaving out ports only used locally (within individual subnets).

Background information on firewall rules

This information applies to setting up firewall rules. If you aren't familiar with the subject, this section provides some generic background information on the main concepts.

Firewall rules

"Opening a port" is not a precise term. You can't just go to a firewall and "open port x." Opening a port is shorthand for setting up a firewall rule. Firewall rules describe what traffic will or will not be allowed through the firewall. Firewall rules don't filter traffic on port number only. Rules can be based on protocols, source and destination port numbers, direction (inbound / outbound), source and destination IP addresses, and other things.

A typical firewall rule looks like this: "allow inbound traffic on TCP port 9535." For using this product, this rule is needed to support remote control. The rule is based on three elements:

1. The protocol (TCP or UDP)
2. The port number
3. The direction (inbound or outbound)

These three elements are required to set up firewall rules.

Source and destination ports, dynamic ports

There are always two ports involved in TCP or UDP communication. Any TCP or UDP packet is from a source port to a destination port. Firewall rules can be based on the source port, the destination port, or both. Ports listed in documents such as this one are always destination ports.

Well-known ports such as 5007 (used by the inventory service) refer to only one side of the communication. The other side of the communication is using a dynamic port. Dynamic ports are assigned automatically by the operating system in the range 1024-5000.

Firewalls and UDP traffic

To allow TCP traffic through a firewall, a single rule is sufficient, such as to allow inbound TCP connections to port 5007. Once the TCP connection is established, data can flow both ways through the connection.

UDP traffic is different because it is connectionless. For example, by default the core server will "ping" devices at UDP port 38293 before starting a task. A firewall rule that allows outgoing UDP packets to port 38293 will allow packets from the core server to a device outside the firewall, but not the device's response packets.

A rule that allows both outgoing and incoming packets to port 38293 won't work either because only one side of the communication is listening on the well-known port. The other side is using a dynamic port. Because the core server's outgoing packets are from a dynamic port to port 38293, the device's response packets are from port 38293 to the same dynamic port, not to port 38293. To allow two-way

communication, a rule is needed that allows UDP packets with source port or destination port = 38293. Such a rule is usually acceptable on the intranet, but not on an external firewall (because it would allow inbound packets to all UDP ports).

For this reason, UDP traffic is usually not considered "firewall friendly". Coming back to the example, there is an alternative to UDP port 38293: TCP port 9595. When managing devices across a firewall, you probably want to configure the product to use the TCP port.

Ports used

Port	Direction	Protocol	Service
31770	console to device, device to core	TCP	communication between console and device
6787	console to device	TCP	communication between console and device
9595	console to device	UDP	discovery
9595	console to device	TCP	agent configuration
623	console to device	UDP	ASF, IPMI discovery
9535	console to device	TCP	remote control

This product needs to discover nodes with the LANDesk agent installed before it can manage them. UDP port 9595 is used for discovery. You can also manually add individual devices to the console, but this still requires the device to respond to a "ping" on UDP port 9595. Communication between the console and the device uses TCP ports 31770 and 6787. Traffic on the latter port is HTTP-based. UDP port 623 is used for ASF (alert standard forum) discovery. In addition, this product uses TCP port 9535 for remote control. IPMI discovery is a linked with ASF discovery and uses the same port (udp/623).

Phase 2: Preparing your databases

This phase focuses on preparing the core database.

In phase 2, you'll learn about:

- Microsoft SQL Server 2000 configuration
- Oracle database configuration
- LANDesk Software support and DBMS issues

Before you begin

Server Manager requires interaction with a database management system (DBMS). Your DBMS server is an integral part of the management domain infrastructure. It handles all of the information the product needs to manage devices in your domains.

The default installation uses a Microsoft MSDE database on your core server.

If you aren't planning on using a default MSDE database on your core server, you need to set up a database before running the product's Setup. During Setup, you'll point to the database that will hold your data.

The database schema also supports these ODBC-compliant DBMSes:

- Microsoft SQL Server 2000 with SP 4
- Oracle8i (8.1.7). Requires Oracle's OLE DB version 8.1.7.3 update.
- Oracle9i

The database being used needs to support the language that the core has been installed to. For example, if the core is installed on a French operating system, the database it is using needs to support French either through a native install of French or through an installed language pack.

All database servers need to have MDAC 2.8 on them. You no longer need to create a database DSN for ODBC.

The deciding factor in selecting a DBMS for your database is the number of managed devices in your product domain. In Phase 1: Designing your management domain, you determined the number of devices in your management domains. Based on that number of devices, you can select the default database (MSDE) or a supported ODBC-compliant DBMS for a larger management domain.

The steps below are for installing the core database. In Oracle, the product uses public synonyms.

For detailed database installation steps
You can view detailed installation steps for each database on the LANDesk Software support Web site: http://www.landesk.com/go/ldmsdbwp.

If you have a preexisting Windows 2000/2003 master domain
Don't install the DBMS to the primary domain controller (PDC). The DBMS should be installed only on a standalone server. You can install the DBMS on the backup

domain controller (BDC) in a small Windows 2000/2003 domain, but it is not recommended.

Microsoft SQL Server 2000 configuration

This product needs the following parameters. These parameters will be set by default if you use a typical install for SQL 2000:

SQL server configuration parameters

- Microsoft SQL 2000 performs self-tuning. You shouldn't need to tune any parameters manually.

Database parameters

- Use the defaults.

Other settings

- Use "sa" or another user aliased into the database as DBO when creating the database.
- Set up database maintenance.

To install the product so that it uses your SQL 2000 database

1. Install the product to the point where you need to choose a database.
2. In the **Choose a Database** page, click **User-supplied database** and then click **Next**.
3. Enter the **Server** and **Database** names, and enter the **User** and **Password** that the product should use to authenticate to the database. You MUST use a user who is aliased into the database as DBO. Don't use "sa" for the login name. Don't use any other user to create or reset the database. If another user attempts to connect to the database and the tables aren't owned by DBO, the user won't be able to see the tables. If you're using an Oracle database, check **This is an Oracle database**.
4. Click **Next** and finish the product install.

SQL maintenance

You must regularly perform maintenance on a Microsoft SQL Server database. Over time, the indexes become very inefficient. If your database queries seem to be running more slowly than normal, updating statistics on all tables within the database can substantially improve query performance. On very large databases, you might want to update statistics daily.

Microsoft SQL maintenance requires the SQLServerAgent service to be running on the SQL server. You may need to set the service to Automatic in the Control Panel Services applet. SQL maintenance won't run unless the SQLServerAgent service is started.

To set up a maintenance task

1. Click **Start | Programs | Microsoft SQL Server | Enterprise Manager**.
2. Click the + next to these folders: **Microsoft SQL Servers**, **SQL Server Group**, **the name of your server**, and **Management**.
3. Right-click **Database Maintenance** and click **New Maintenance Plan**.
4. In the **Database Maintenance Plan** dialog, click **Next**.
5. In the **Select Databases** dialog, select **These databases** and select the checkbox for your database. Click **Next**.
6. In the **Update Data Optimization Information** dialog, click **Reorganize data and index pages**.
7. Set the **Change free space per page percentage to** option to **10**.
8. Click the **Change** button next to the **Schedule** window.
9. In the **Edit Recurring Job Schedule** dialog, select the schedule you want for maintenance. We suggest you perform the maintenance at least weekly at a time when there will be minimal database activity.
10. Click **OK**.
11. In the **Database Integrity Check** dialog, select these options: **Check database integrity** and **Include indexes,** and click **Next**.
12. In the **Specify the Database Backup Plan** dialog, specify your own backup schedule and click **Next**.
13. In the **Specify the Transaction Log Backup Plan** dialog, specify your own backup schedule and click **Next**.
14. In the **Reports to Generate** dialog, select the **Write report to a text file in directory** option and click **Next**.
15. In the **Maintenance Plan History** dialog, select the **Write history to the msdb.dbo.sysdbmaintplain_history table on this server** option.
16. Set the **Limit rows in the table to** option to **1000**.
17. Click **Next**.
18. In the **Completing the Database Maintenance Plan** dialog, enter a **Plan name** and click **Finish**.

Oracle database configuration

The default Oracle client installation installs Apache, disables IIS, and makes Apache the default web server. The Web console requires IIS. If you're doing a full Oracle client installation on the core server, make sure you disable the Apache feature in the client installer.

After installing an Oracle database, do the following:

1. Create a tablespace for the product's Setup to use.
2. Create a user with the following system rights for the product's Setup to use:

    - Create Procedure
    - Create Sequence
    - Create Session
    - Create Table
    - Create Trigger
    - Create Type
    - Create View
    - Force Transaction

- Unlimited Tablespace

3. Set the user's default tablespace to the tablespace created for product use.
4. On the core server, create a TNS entry for the Oracle instance.

Oracle performance tuning suggestions and scripts

Like any DBMS, Oracle should be tuned to help increase performance. The first step in increasing performance is to make sure sufficient hardware is allocated for the Oracle instance.

If your database queries seem to be running more slowly than normal, updating statistics on the tables and indexes in the database can substantially improve query performance. On very large databases, you might want to update statistics daily.

Miscellaneous Oracle issues

The following sections contain specific issues that you should review to get optimal performance when using an Oracle database with this product.

TNS Names

Use Oracle's SQL Net Easy Configuration tool to create a TNS entry on the core server that points to the physical location of the Oracle database. The configuration tool adds an entry into $ORACLE_HOME/Network/ADMIN/TNSNames.ora file.

If services fail to start using Oracle

If the LANDesk services are failing to start and checking the event log shows errors about “Adapter initialization failures” or “Adapter Authentication failures,” change the following file:

$ORACLE_HOME/network/admin/sqlnet.ora

Change:

SQLNET.AUTHENTICATION_SERVICES = (NTS)

To:

SQLNET.AUTHENTICATION_SERVICES = (NONE)

Using Oracle 9.2.0.1 with the Web console

If you use an Oracle 9.2.0.1 database, there is an Oracle install issue that doesn't set the proper permissions for authenticated users (which IIS uses). Follow these steps to fix it.

1. Log in to Windows as a user with administrator privileges.
2. Launch Windows Explorer from the Start menu and navigate to the ORACLE_HOME folder. This is typically the "Ora92" folder under the "Oracle" folder (i.e. D:\Oracle\Ora92).
3. From the ORACLE_HOME folder's shortcut menu, click **Properties**.
4. Click the **Security** tab.

5. In the **Name** list, click **Authenticated Users**.
6. In the **Permissions** list under the **Allow** column, clear the **Read and Execute** option.
7. Re-check the **Read and Execute** option under the **Allow** column (this is the box you just cleared).
8. Click **Advanced** and, in the **Permission Entries** list, make sure you see the **Authenticated Users** listed there with Permission = Read & Execute and Apply To = This folder, subfolders and files. If this isn't the case, edit that line and make sure the **Apply onto** box is set to **This folder, subfolders and files**. This should already be set properly, but it's important that you verify this.
9. Click **OK** until you close out all of the security properties windows.
10. Reboot your server to make sure that these changes have taken effect.

LANDesk Software support and DBMS issues

LANDesk Software customer support is committed to helping you resolve database issues for this product. Some issues may require additional assistance from the database vendor or through an approved third party. The database support that LANDesk Software customer support won't provide includes, but is not limited to, the following:

- Configuring the DBMS with additional parameters for performance or other reasons
- Creating scripts
- Configuring an existing DBMS installation to work with this product
- Restricting rights or performing other user maintenance
- Backing up the databases
- Repairing corrupt databases

If you call LANDesk Software customer support, support personnel will attempt to do the following:

- Isolate the problem
- Verify that the specified DBMS parameters are correct
- Verify that the product is working correctly
- Verify that the product works with MSDE

If, at this point, the DBMS still doesn't work, you may need to either reinstall the DBMS or resolve the issue through other means.

Phase 3: Installing the core

This phase focuses on installing the core server. During this installation, you'll use the information you recorded in Phase 1: Designing your management domain. If you haven't completed all the tasks in the preceding phases, do so before beginning this phase.

In phase 3 , you'll learn about:

- Installing the core server
- Activating the core server
- Managing databases after installation

The installation of the components outlined in this phase requires about 30-60 minutes. If you're creating multiple domains, we recommend that you successfully complete the installation and deployment of one management domain before creating another.

Make sure you review the system requirements described in Phase 1: Designing your management domain.

Installing the core server

To install the core server

Before starting the install, it is recommended that you close other applications and save any open files. At the Windows 2000/2003 server you've selected to be your core server:

1. Insert the product CD into the CD-ROM drive or run AUTORUN.EXE from your installation image. The Autorun feature will display a Welcome screen.
2. Click **LANDesk® Server Manager** or **LANDesk® Management Suite with LANDesk® Server Manager**.
3. The system requirements checker runs to verify that the server meets minimum system requirements. Make sure all requirements pass. If any do not pass, click **Fail** on the failed requirement's link for links or information regarding installing the failed requirement.
4. Click **Install now** to run the Setup program.
5. Select the language you want Setup to install. Click **OK**.
6. A Welcome screen appears. Click **Next** to continue.
7. On the License Agreement screen, if you agree click **I accept the terms in the license agreement** to continue. Click **Next**.
8. Accept the default destination folder, or specify a custom destination folder, and click **Next**. The destination folder path cannot contain double-byte characters. If you change this folder, remember to substitute your path for any paths you see in the product documentation.
9. Select where the core server should store device information, either **Add LANDesk tables to a database** or a user-supplied database that you've already configured. Click **Next**.

10. Enter an MSDE database password. Remember this password or write it down. Click **Next** to continue.

10. Enter an organization and certificate name for the core server's security certificate. This information helps name and describe the certificate. Click **Next**.
11. If you are installing Management Suite with Server Manager, and you want to create a non-Management Suite user who can view reports, enter a user name and password for the user. This user will be a member of the LANDesk Reports group.
12. If you are installing Management Suite
13. On the **Ready to Install** page, click **Install**. The product will start installing.
14. The **Installation Wizard Completed** dialog appears when Setup is done.
15. Click **Finish**.
16. Setup will prompt you to restart the server. You must click **Yes** to finish Setup. When the server restarts, you'll notice after you log in that Setup will run for a few more minutes while it finishes the installation. Setup won't prompt you for any more information during the first reboot.

When installing an MSDE core database on a Windows 2003 Server, Windows may interrupt the Setup and ask if it's OK to open SETUP.EXE. If you see this prompt, click **Open** or the product won't be installed correctly.

Activating the core server

LANDesk Software uses a central licensing server to help you manage your core server's product and device licenses. To use the LANDesk products, you must obtain from LANDesk a user name and password that will activate the core server with an authorized certificate. Activation is required on the core server before you can use LANDesk products on that server. You can activate the core server either automatically by the Internet or manually by e-mail. You may need to reactivate a core server in the event that you significantly modify its hardware configuration.

On a periodic basis, the activation component on the core server will generate data regarding:

- The precise number of devices you're using
- The non-personal encrypted hardware configuration
- The specific LANDesk Software programs you're using (collectively, the "server count data")

No other data is collected or generated by the activation. The hardware key code is generated on the core server using non-personal hardware configuration factors, such as the size of the hard drive, the processing speed of the computer, and so on. The hardware key code is sent to LANDesk in an encrypted format, and the private key for the encryption resides only on the core server. The hardware key code is then used by LANDesk Software to create a portion of the authorized certificate.

After installing a core server, use the Core Server Activation utility (**Start | All Programs | LANDesk | Core Server Activation**) to either activate it with a LANDesk account associated with the licenses you've purchased or with a 45-day evaluation license. The 45-day evaluation license is for 100 devices. Any time you

install product agents on a server operating system, such as Windows 2000 Server or HP-UX, that installation consumes a product license for a server.

You can switch from a 45-day evaluation to a paid license at any time by running the Core Server Activation utility and entering your LANDesk Software user name and password.

Each time the server count data is generated by the activation software on a core server, you need to send the server count data to LANDesk Software, either automatically by the Internet or manually by e-mail. If you fail to provide server count data within a 30-day grace period after the initial server count verification attempt, the core server may become inoperative until you provide LANDesk with the server count data. Once you send the server count data, LANDesk Software will provide you with an authorized certificate that will allow the core server to work normally once again.

After you've activated a core server, use the console's **Preferences | License** dialog to view the products and the number of authorized servers purchased for the account the core server authenticates with. You can also see the date the core server will verify server count data with the central licensing server. The core server doesn't limit you to the number of authorized servers you purchased. You can view information about the licenses you're using by visiting the LANDesk Software licensing site at www.landesk.com/contactus.

About the Core Server Activation utility

Use the Core Server Activation utility to:

- Activate a new server for the first time
- Update an existing core server or switch from a trial-use license to a full-use license
- Activate a new server with a 45-day trial-use license

Start the utility by clicking **Start | All Programs | LANDesk | Core Server Activation**. If your core server doesn't have an Internet connection, see Manually activating a core or verifying the server count data later in this section.

Each core server must have a unique authorized certificate.

Periodically, the core server generates server count verification information in the "\Program Files\LANDesk\Authorization Files\LANDesk.usage" file. This file gets sent periodically to the LANDesk Software licensing server. This file is in XML format and is digitally signed and encrypted. Any changes made manually to this file will invalidate the contents and the next usage report to the LANDesk Software licensing server.

The core communicates with the LANDesk Software licensing server via HTTP. If you use a proxy server, click the utility's **Proxy** tab and enter your proxy information. If your core has an Internet connection, communication with the license server is automatic and won't require any intervention by you.

Note that the Core Server Activation utility won't automatically launch a dial-up Internet connection, but if you launch the dial-up connection manually and run the activation utility, the utility can use the dial-up connection to report usage data.

If your core server doesn't have an Internet connection, you can verify and send the server count manually, as described later in this section.

Activating a server with a LANDesk Software account

Before you can activate a new server with a full-use license, you must have an account set up with LANDesk Software that licenses you for the LANDesk Software products and number of server licenses you purchased. You will need the account information (contact name and password) to activate your server. If you don't have this information, contact your LANDesk Software sales representative.

To activate a server

1. Click **Start | All Programs | LANDesk | Core Server Activation**.
2. Click **Activate this core server using your LANDesk contact name and password**.
3. Enter the **Contact name** and **Password** you want the core to use.
4. Click **Activate**.

Activating a server with a trial-use license

The 45-day trial-use license activates your server with the LANDesk Software licensing server. Once the 45-day evaluation period expires, you won't be able to log in to the core server, and it will stop accepting inventory scans, but you won't lose any existing data in the software or database. During or after the 45-day trial use license, you can rerun the Core Server Activation utility and switch to a full activation that uses a LANDesk Software account. If the trial-use license has expired, switching to a full-use license will reactivate the core.

To activate a 45-day evaluation

1. Click **Start | All Programs | LANDesk | Core Server Activation**.
2. Click **Activate this core for a 45-day evaluation**.
3. Click **Activate**.

Updating an existing account

The update option sends usage information to the LANDesk Software licensing server. Usage data is sent automatically if you have an Internet connection, so you normally shouldn't need to use this option to send server count verification. You can also use this option to change the LANDesk Software account the core server belongs to. This option can also change a core server from a trial-use license to a full-use license.

To update an existing account

1. Click **Start | All Programs | LANDesk | Core Server Activation**.
2. Click **Update this core server using your LANDesk contact name and password**.
3. Enter the **Contact name** and **Password** you want the core to use. If you enter a name and password that's different than the one used to originally activate the core, this switches the core to the new account.
4. Click **Activate**.

Manually activating a core or verifying the server count data

If the core server doesn't have an Internet connection, the Core Server Activation utility won't be able to send server count data. You'll then see a message prompting you to send activation and server count verification data manually through e-mail. E-mail activation is a simple and quick process. When you see the manual activation message on the core, or if you use the Core Server Activation utility and see the manual activation message, follow these steps.

To manually activate a core or verify the server count data

1. When the core prompts you to manually verify the server count data, it creates a data file called activate.xml in the "\Program Files\LANDesk\Management Suite" folder. Attach this file to an e-mail message and send it to licensing@landesk.com. The message subject and body don't matter.
2. LANDesk Software will process the message attachment and reply to the mail address you sent the message from. The LANDesk Software message provides instructions and a new attached authorization file.
3. Save the attached authorization file to the "\Program Files\LANDesk\Authorization Files" folder. The core server immediately processes the file and updates its activation status.

If the manual activation fails or the core can't process the attached activation file, the authorization file you copied is renamed with a .rejected extension and the utility logs an event with more details in the Windows Event Viewer's Application Log.

Logging into the console

After you've rebooted the core server and Setup has finished, and the core has been activated, start the console by opening a browser and typing the server's address in the following format: *http://servername/ldsm*. Once the console starts, you'll see the console login window. You may be prompted to enter the credential of the account that installed LDSM in order to log in. Only members of the LANDesk Management Suite group on the core server can log on. By default, Setup added the user you were logged in as when you installed the core to the LANDesk Management Suite group. If you want other users to be able to access the console, add them to this group.

After you install the Web console server, the first time you launch the console in a browser it may take up to 90 seconds to display. This delay happens because the server has to do a one-time compile of some Web console code. The console will launch much faster after the first time.

This product has role-based administration, where you can configure what devices and features other console users have access to. For more information, see "Role-based administration" in the *User's Guide*.

Managing databases after installation

Installing a rollup core

You can use a rollup core to combine the data from multiple core servers. Rollup cores allow you to exceed the core limit of approximately 10,000 devices. You must schedule rollup core updates to synchronize the rollup core database with each core server's core database. Using the console, you can then manage devices in the rollup core using queries, software distribution, remote control, and the other features.

Before installing a rollup core, you need to have configured an additional Oracle or SQL Server rollup database server as described in "Phase 2: Preparing your databases." The rollup option will prompt you for information about the database you've set up.

To install a rollup core

1. Set up a rollup core server and database. Install the database as described in Phase 2: Preparing your databases.
2. Log in to the rollup core server with an account that has administrator rights.
3. Map a drive to the LDMAIN share on the core server.
4. From the Install\Rollup Core folder, run the Rollup Core shortcut.
5. Proceed through Setup, and make sure you select the Rollup core component.
6. Finish Setup.

Using rollup databases

The database Rollup Utility (DBROLLUP.EXE) enables you to take multiple source core databases and combine them into a single destination core rollup database. A core server database can support about 10,000 devices, and the rollup core device limit depends on your hardware and acceptable performance levels. The source database can be from either a core server or a rollup core server.

The system requirements for a destination database may be substantially greater than the system requirements for a standard database. These requirements can vary considerably depending on your network environment. If you need more information about hardware and software requirements for your destination database, contact your LANDesk Software support representative.

Setup installs the database Rollup Utility automatically with the rollup core. The Rollup Utility uses a pull mechanism to access data from cores you select. For database rollups to work, you must already have a drive mapped to each core you want the Rollup Utility to get data from. The account you connect with must have rights to read the core server's registry.

The Rollup Utility checks with a registry key on the core server for database and connection information (HKLM\SOFTWARE\LANDesk\ManagementSuite\Core\Connections\local) and uses that key's information to access the database associated with each core you add to the Rollup Utility. For Oracle databases, the TNS definition on the server you're running the Rollup Utility from must match the TNS definition on the core server the utility is accessing.

You can use the rollup utility to select the attributes you want rolled up from the cores. The attribute selections you make apply to all cores. Limiting the number of attributes shortens the rollup time and reduces the amount of data transferred during rollups. If you know you won't be querying on certain attributes, you can remove them.

The Rollup Utility always rolls up the selected attribute data and Software License Monitoring data. You can't customize the Software License Monitoring rollup. Rollup also doesn't include any queries or scopes you've defined. Any console users with rights to the rollup database have access to all data within that database.

Once you've added the core servers you want to roll up and the attribute list for those servers, you can click **Schedule** to add a scheduled rollup script for each core server. From a web console, you can then schedule these rollup scripts to run at the time and interval you want. Rollup scripts are only visible from the web console and reside on the rollup core.

To launch the Rollup Utility

1. On a rollup core, run the Rollup Utility (\Program Files\LANDesk\ManagementSuite\dbrollup.exe).
2. Select an existing rollup core server to manage from the list, or click **New** to enter the name of a new rollup core server. Note that you must enter the core server name, not the database name.
3. Once you select a rollup core, the **Source cores** list shows cores you've configured to roll up to the selected rollup core.

To configure the attributes that you want to roll up

1. From the Rollup Utility, select the rollup core you want to configure.
2. Click **Attributes**.
3. By default, all database attributes are rolled up. Move attributes from the **Selected Attributes** column to the **Available Attributes** column that you don't want to roll up.
4. Click **OK** when you're done. Moving attributes to the **Available Attributes** column deletes associated data from the rollup database.

To configure the source core servers for a rollup core

1. From the Rollup Utility, select the rollup core you want to configure.
2. Once you select a rollup core, the **Source cores** list shows cores you've configured to roll up to the selected rollup core. Click **Add** to add more cores or select a core and click **Delete** to remove one. **WARNING:** Clicking **Delete** immediately removes the selected core and all of that core's data from the rollup core database.

To schedule database rollup jobs from the web console

1. From the Rollup Utility, select the **Rollup core** you want to configure.
2. In the **Source cores** list, select the cores you want to schedule for rollup and click **Schedule**. If you don't select any cores, by default all cores in the list will be scheduled when you click **Schedule**. Clicking **Schedule** adds a rollup

script for the selected core to the selected rollup core. If you select multiple cores, they will be scheduled as one job and will be processed one at a time.

3. You won't be able to log into a rollup core server from the web console until at least one core has been rolled up to it. Make sure you use the Rollup Utility's **Rollup** button to manually roll up at least one core.
4. From a Web console, connect to the rollup core server.
5. In the left navigation pane, click **Scheduled tasks**.
6. Click the rollup script you want to schedule. The script names begin with the source core name followed by the destination rollup core name in parentheses. Click **Edit**.
7. Select when you want the roll up to happen and whether it should automatically reschedule or not. Make sure there isn't more than one core being rolled up at a time. Click **Save**.

You can view the rollup task status in the **Status** column. The column displays "All Completed" when the task is finished. You can also view the status of the task in the Windows Event Viewer.

Only one rollup can be processed at a time. A scheduled rollup will fail if another rollup is already in progress. When scheduling rollups, allow enough time between rollups that there won't be any overlap. If the rollup times are hard to predict, it's best to schedule all the rollups in a single job. Do this by selecting multiple cores before clicking **Schedule**. This way, the rollups are handled one at a time automatically.

Increasing the rollup database timeout

With large rollup databases, the web console's query editor may time out when it tries to display a large list, such as the Software Package Name list. When this happens, the list you are trying to display won't show any data. If you experience timeouts you need to increase the database timeout value. This needs to be done wherever the IIS service or the Web console server is being installed. Add a new DWORD, Timeout, with a decimal value of 1800 at the following registry key.

`HKEY_LOCAL_MACHINE\SOFTWARE\LANDesk\ManagementSuite\Core`

This value is in seconds. You can adjust this value based on your query types and database performance. Stop and restart IIS for the change to take effect.

About the Rollup Utility

Use the database Rollup Utility (run from the rollup core) to manage data rollups from core servers.

- **Rollup core:** You can manage multiple rollup cores from the Rollup Utility. Select the core you want to manage. You first must have a drive mapped to each rollup core.
- **New:** Click to add a new rollup core that you want to manage. You first must have a drive mapped to the rollup core you're adding. Enter the rollup core's computer name and click **OK**.
- **Attributes:** Click to select the attributes you want rolled up. The attributes list is global for all core servers the selected rollup core uses. Move individual attributes or attribute trees from the **Selected Attributes** column (these attributes will be rolled up) to the **Available Attributes** column (these attributes won't be rolled up).

- **Reset database:** Click to reset the selected rollup database. This deletes all data and rebuilds all tables.
- **Add:** Click to add a core that you want to include data from in the selected rollup core.
- **Delete:** Click to remove the selected core and its data from the selected rollup core's database. **WARNING:** This option deletes the selected core's data when you click **OK**. Data from other core servers remains in the rollup database.
- **Schedule:** Click to add a rollup script for the selected core. If you don't have a core selected in the **Source Cores** box, this option creates rollup scripts for all cores in the **Source Cores** box.
- **Rollup:** Click to do an immediate rollup from the selected core. You must have a core selected for this option to be available.
- **Close:** Click to close the Rollup Utility.

Rollup database link configuration

The following steps describe the configuration of database links in all four possible rollup scenarios.

Oracle to Oracle

Configuring the Oracle database

The TNSNames.ora file on the database server in which your rollup database exists must contain an entry for your core server database.

1. For an Oracle 9i* database, within the Enterprise Manager Console, log in to your database. **Expand Distributed**.

   Or

   For an Oracle 81* database, within the Enterprise Manager Console, log in to your database. **Expand Schema** and your rollup Schema.

2. From the Database Links item's shortcut menu, click **Create**.
3. In the **Name** field, type the name for your database link.

   Note: In the command above, LDMS_LINK is the name of the link. If the AR database is using Oracle8i, the link name must match the TNS name of the remote server. If the AR database is using Oracle 9i, the link name can be any name that is not already in use or is reserved. The installation will prompt you for this information.

4. Select **Fixed User** and enter the information and password for the core server's database.
5. In the **Service Name** field, enter the TNSNames.ora (such as …NetAlias) entry that refers to your core server database.
6. Click **Create**.
7. Double-click the newly-created link and click the **Test** button You should receive a message that states the link is active. You can also test the link by logging into the rollup database and issuing the following command:

   ```
   Select count(*) from computer@linkname;
   ```

If it comes back with the correct number of computers scanned into your core server, the link is set up correctly.

SQL Server to SQL server

Configuring the SQL Server*database

1. Open the SQL Server Enterprise Manager.
2. Expand the server and click **Security**.
3. From the Linked Servers item's shortcut menu, click **New Linked Server**.
4. On the **General** tab, do the following:
    1. Linked Server: Enter a unique name for this database link (for example, LDMS core server1 link)
    2. Choose **Other data source**
    3. Select **Microsoft OLE DB Provider for Microsoft SQL Server**
    4. Product Name: Leave blank
    5. Data source: Enter the name the database server containing the core database.
    6. Provider string: Enter your provider string. (for example, SQL Server provider=SQLOLEDB.1,user id=<username for the core server's database>)
    7. Catalog: Enter the physical name of your core server's database (for example, lddb)
5. On the **Security** tab, select **Be made using this security context** and enter the username and password for the core server's database, then click **OK**.
6. Open SQL Query Analyzer and issue the following command:

```
Select.count(*) from [Link name].[table-owner name].Computer
```

Using the values above, this query will appear as:

```
Select count(*) from [LDMS Core Server1
link].[lddb].[dbo].Computer
```

If the correct count comes back, your link is set up correctly.

SQL Server rolling to Oracle

Configuring SQL Server* to rollup to Oracle

In order to roll SQL Server to Oracle, you must capitalize all column names in the production SQL database. If you want a utility to do this for you, call LANDesk custom support.

Install Heterogeneous Services for Oracle

1. Using the Oracle Universal Installer, Install the Transparent Gateway for SQL.
2. Edit <oracle home>\rdbms\admin\caths.sql on the Oracle DBMS server so that the two lines that call PRVTHS.PLB and DBMSHS.SQL point to the appropriate directory on Oracle DBMS server.
3. Execute CATHS.SQL using SQL Plus by logging in to SQL Plus and at the prompt typing @@ORACLE_HOME/RDBMS/ADMIN/CATHS.SQL.

The following error may appear at the end script execution.

068: existing state of packages has been discarded

063: package body “LDPROD.DBMS_HS_UTL” has errors

508: PL/SQL: could not find program unit being called

512: at “LDPROD.DBMS_HS”, line 629

403: No data found

512: at line 6

This error can be caused by an outdated version of JDBC drivers that exists on the Oracle DBMS server. Please call Oracle for troubleshooting and further investigation of your installation if you receive errors during the execution of CATHS.SQL or the scripts that it may call.

To create a UDL file on the core server pointing to the SQL DBMS

1. Right-click the desktop, click **New** > **Text document**. Save it as <core server name>.udl. Double-click the .udl file and the **Data Link Properties** dialog displays.
2. On the **Provider** tab, click Microsoft OLE DB Provider for SQL Server.
3. On the **Connections** tab, fill in the database information for the core server’s SQL Server database. Click **Allow Saving Password** to save the password information to the UDL file.
4. Click **OK** to save the connection information. When prompted to save the password, click **Yes**.

To create a SID on the Oracle server pointing to the SQL server

1. Copy ORACLE_HOME/hs/admin/inithsoledb.ora and rename it to init<core server name>.ora. Copy the UDL file created on the core to ORACLE_HOME/hs/admin.
2. Edit the init<core server name>.ora file. Change the HS_FDS_CONNECT_INFO= line to reflect the path to your UDL file on the Oracle DBMS server. Leave the %_TRACE_LEVEL=0 parameter equal to 0.
3. Save the init file and close it.
4. Create a listener pointing to the SQL Server by editing the Listener.ora and TNSNAMES.ORA files under ORACLE_HOME/Network/Admin on the Oracle DBMS server.

Sample Entry for TNSNAMES.ORA

<core server name>=

(DESCRIPTION=

ADDRESS_LIST=

ADDRESS=(PROTOCOL=TCP)(HOST=<Oracle DBMS server>name)(PORT=1521))

)

(CONNECT_DATA=

(SID=<name of core server>)

)

(HS=OK)

)

Sample entry for LISTENER.ORA

(SID_DESC=

(GLOBAL_DBNAME=<name of core server>)

(PROGRAM=hsolesql)

SID_NAME=<name of core server>)

(Oracle_HOME=E:\Oracle\ora92)

)

6. Restart the Listener Service on the Oracle DBMS server so that the Oracle server will now be able to connect to the SQL Server using OLEDB and Transparent Service.

Create a Database Link using the core server-named SID

Use the Core Server Name entry in TNSNames.ora file for the Heterogeneous Services link in order to create your link to your SQL Server production database.

1. For your Oracle 9i database, within the Enterprise Manager console, log in to your database. Expand **Distributed**. For an Oracle 8i database, within the Enterprise Manager console, log into your database. Expand **Schema** and your rollup Schema.
2. From the Database Links item's shortcut menu, click **Create**.
3. In the **Name** field, enter a name for your database link.
4. Choose **Fixed User** and enter a username and password for the core server's database.
5. In the **Service Name** field, enter the TNSNames.ora (i.e, Net Alias) entry that refers to your core database.
6. Click **Create**.
7. Double-click the newly created link and click the **Test** button. You should get a message that says your link is active. You can also test your link by logging into the rollup database and issuing the following command:

```
Select count(*) from computer@linkname;
```

If it comes back with the correct number of computers scanned into your core server, your link is set up correctly.

8. You can also create your link by logging into SQL Plus for Oracle and typing the following SQL statement:

```
create database link "<core server name(this will be the
linkname)>"

connect to "<sql user name>" identified by "<password>" using
'<core server name(this is the SID name)>':
```

Oracle rolling to SQL Server

Configuring Oracle to rollup to SQL Server

Because of a known issue in the Oracle 9i client, it is impossible to use DBROLLUP.EXE to roll an Oracle production database to an SQL Server rollup database using an Oracle 9i client.

It is possible to use that Oracle 9i client to roll an Oracle 9i database to an SQL server. Currently, the Oracle 10G client is not supported in conjunction with LANDesk Management Suite. However, it can be used though in conjunction with DBROLLUP.EXE in order to allow rollup of an Oracle database to SQL Server based upon the following limitations:

1. The Oracle 10G client cannot be installed on any server that houses a LANDesk core server, LANDesk additional console, or LANDesk web console server.
2. The Oracle 10G client can only be used to point to an existing supported LANDesk production Oracle 9i database.

To create a link to the Oracle database in SQL Server

1. Install the Oracle 10G on the rollup server.
2. Create an Oracle Net Alias to the production Oracle database. The Alias name must be the same as the Alias name used on the core server that uses that database.
3. Open SQL Server Enterprise Manager.
4. Expand your server and click **Security**.
5. From the Linked Servers item's shortcut menu, click **New Linked Server**.
6. On the **General** tab, do the following:
    1. Linked Server: Enter a unique name for this database link (for example, LDMS Core Server1 Link).
    2. Choose **Other data source**.
    3. Select **Oracle Provider for OLE DB**.
    4. Product Name: Leave blank.
    5. Data source: Enter the name the database server containing the core database.
    6. Provider string: Enter your provider string. For instance: Oracle provider=ORAOLEDB.ORACLE1.
7. On the **Security** tab, do the following:
    1. Select **Be made using this security context** and enter the username and password for the core server's database, then click **OK**.
    2. Open SQL Query Analyzer and issue the following command:

```
Select count(*) from [Link name]..[Oracle User Name].COMPUTER

Using the values above, this query would appear as:

Select count(*) from [LDMS Core Server1 Link]..[Oracle User Name].COMPUTER

If the correct count comes back, your link is set up correctly.
```

Running CoreDbUtil to reset, rebuild, or update a database

The CoreDbUtil.exe utility, in the core server's \Program Files\LANDesk\ManagementSuite folder, creates all the tables, indexes, and constraints needed to use the core database. Before running CoreDbUtil.exe, you must install your database as described in Phase 2: Preparing your databases or the table creation may fail. CoreDbUtil.exe looks for registry keys on the core server to determine the core database connection information.

The Core Database Management Utility (COREDBUTIL.EXE) performs the following functions:

- Creates a new core database during installation.
    - The product performs the ResetDatabase operation in silent mode after storing database connection information to the registry and providing all needed files.
    - The product performs the PublishSoftwareConfiguration operation after the ResetDatabase operation.
    - The product performs the UpdateCannedReports operation after the PublishSoftwareConfiguration operation.
- Resets an existing core database.
    - Drops all tables, and rebuilds the database from scratch using DATAMART.XML.
    - Rebuilds Vulnerability scanning database tables.
- Builds Components in an existing core database.
    - Updates the schema (specifically to include column additions) from the METADATA.XML. This is not destructive to existing data.
- Publishes Software Configuration in an existing core database.
    - Adds Software Configuration info using DEFAULTS.XML and LDAPPL3.TEMPLATE to generate LDAPPL3.INI, LDAPPL3.BAK, LDAPPL3.LDZ, LDAPPL3.PAT, LDAPPL3.PAZ, and LDAPPL3.RESET.
- Updates Canned Reports in an existing core database.
    - Adds Canned Reports to Database using CANNEDREPORTS.XML.
- Updates Devices Display Names in an existing core database.
    - Updates the "Display Name" field in an existing core database for all devices in that database. The core must have a valid license (must be activated) for this operation.
- Modifies a core database to support the Patch Management module.
    - Patch Management installation performs the PatchManagement operation after providing any needed files.

Each of these first-level bullets is represented by a button on the utility interface.

Command line parameters

To run COREDBUTIL

1. From the ldmain share on the core server, run COREDBUTIL.EXE. Use the switches listed below.
2. After COREDBUTIL connects to the database, select the option you want.
3. Wait until the status is **Finished**. Depending on the database size and the task you chose, this could take a few minutes or several hours.

Operation switches

Only one operation switch may be specified, if more than one is specified, the first one found in the following order is used.

/xml=<filename>

Lets you specify an xml file on which to perform an operation. If this switch is not included, it defaults to Datamart.xml. For example, /xml=datamartpm.xml removes all vulnerability definitions.

/UpdateDisplayNames

This switch causes the Display Name of devices to be updated. Operation performed is equivalent to Update Display Names button in the UI.

/BuildComponents

This switch causes any missing database components in the specified xml file (see /xml=<filename> switch) to be built. Existing Data is preserved. Operation performed is equivalent to Build Components button in the COREDBUTIL dialog.

/ResetDatabase

This switch causes the database tables in the specified xml file (see /xml=<filename> switch) to be dropped before the components are rebuilt. It is the default switch when the /Silent switch is used, if no Option switch is specified. Operation performed is equivalent to Reset Database button in the COREDBUTIL dialog.

/PublishSoftwareConfiguration

This switch publishes the software configuration list using dEFAULTS.XML and LDAPPL3.TEMPLATE to generate LDAPPL3.INI, LDAPPL3.BAK, LDAPPL3.LDZ, LDAPPL3.PAT, LDAPPL3.PAZ, and LDAPPL3.RESET. Operation performed is equivalent to Publish App List button in the COREDBUTIL dialog.

/UpdateCannedReports

This switch causes the canned or predefined reports to be imported into the database using CANNED REPORTS.XML. Operation performed is equivalent to Update Reports button in the COREDBUTIL dialog.

/NukeDatabase

Drop the entire database. There is no equivalent button in the UI.

The COREDBUTIL.EXE utility, in the core server's \Program Files\LANDesk\ManagementSuite folder, creates all the tables, indexes, and constraints needed to use the core database. Before running COREDBUTIL.EXE, you must install your database as described in Phase 2: Preparing your databases of this Deployment Guide or the table creation may fail. COREDBUTIL.EXE looks for registry keys on the core server to determine the core database connection information.

Phase 4: Deploying the primary agents to devices

In phase 4, you'll learn about phased deployment. *Deployment* is the process of expanding your management capabilities to the devices you want to include in your management domain.

You deploy this product by loading LANDesk agents and services onto devices. This allows you to manage them from a single, central location.

In Phase 4 you'll learn about:

- The phased deployment strategy
- Checklist for configuring devices
- Deploying to Windows 2000/2003 servers
- Deploying to Linux servers
- Deploying to devices using software distribution packages
- Understanding the device configuration architecture

The phased deployment strategy

Phased deployment is based on three principles:

1. Deploy the components that have the least impact on your existing network first; then progress to the components that have the most impact.
2. Confirm that the functionality of each deployed component is stable on all device types before continuing to the next stage.
3. Proceed through the deployment of the product in well-planned phases, rather than deploying all components at once, which may complicate any required troubleshooting.

If you've completed the first three phases, you're ready to begin this final phase of deploying the product to your devices.

Checklist for configuring devices

To configure devices, use the following guidelines:

- **Push-based configuration**: Use agent configuration to define a device configuration. Target the desired devices, then schedule a task to push the configuration to the devices. See Configuring agents in the *User's Guide*.
- **Manual configuration**: Map a drive to the core server's LDLogon share and run SERVERCONFIG.EXE, the server configuration program. The components that are deployed to the device must be selected interactively.
- **Package**: Create a self-extracting device installation package.

Obviously, manual configuration is not practical in a large environment when installing to and configuring devices. In most cases, you will push agents to your managed devices.

Regardless of the way you're configuring devices, make sure you've used the **Agent configuration** tab in the console to create the device configuration you want to deploy.

For Windows XP Professional SP2 or 2003 SP1 systems, the settings below require manual configuration of the firewall in order for full product functionality:

Managed Servers:

File and Printer Sharing - TCP 139, 445; UDP 137,138 (Push won't work without this)

Software distribution - TCP 9594, 9595 (Push won't work without this)

Advanced - ICMP - "Allow incoming echo request" (Cannot be discovered if this is not enabled.)

Core Server:

Inventory – 5007

To do so, click **Start** | **Control Panel** | **Security**.

Particularly in bandwidth-sensitive environments, you should deploy the most important or most heavily used agents first, then install all software together as you verify that your system is stable. Any deployment uninstalls all existing agents. For example, if you deploy remote control, and want to add vulnerability to this configuration, you must install remote control and vulnerability.

For the initial deployment, we recommend that you first deploy the primary agents:

- Standard LANDesk Agent (required)
- Software distribution
- Vulnerability scanner
- Remote control
- Monitoring

This product comes with a default server configuration that includes all of the above agents. A default Linux configuration also comes with the product. It includes the standard LANDesk agent, vulnerability scanner, and monitoring agents.

You can add the other agents to the default configurations or create new configurations. Please note that the process of deploying agents is not cumulative; to deploy a new agent to a configuration, you must include it with all previous agents you want in the configuration.

To create the primary agent device configuration

1. In the left navigation pane, click **Agent configuration**.
2. Click **New**.
3. Type a name for the new configuration in the **Configuration name** box.

Type a name that describes the configuration you're working on, such as DBServer or Executive Office Server. This can be an existing configuration name or a new one.

4. Select **Linux** or **Microsoft Windows** or **HP-UX**.
5. To manage IPMI-enabled servers without installing LANDesk software agents, check **IPMI BMC-only configuration** if the configuration is for IPMI-compliant servers, then click **OK**.
6. Select the configuration you just created, and click **Edit**.

In the tabs, some options might be dimmed because they do not apply to the configuration you chose. For example, remote control is not configurable for a Linux configuration because SSH is used for remote access. If you select an IPMI BMC-only Windows configuration, there are no configurable options.

7. In the **Agent** tab, select the agents you want to deploy.

- **All:** Installs all agents on the selected device.
- **Remote control:** Installs the Windows remote control agent on the selected device. This lets you use a special application-level version of remote control for extra reliability. By running remote control at the application level instead of the driver level, the device won't be as vulnerable to remote control problems.
- **Remote Control mirror driver:** Installs the remote control mirror driver, which reduces the amount of time required to see the targeted machine's desktop.
- **Vulnerability scanner:** Installs the vulnerability scanner. With this agent installed, you can configure how the scanner runs to detect vulnerabilities and available updates.
- **Software distribution:** Installs the SWD agent on the selected device. This allows for automating the process of installing software applications or distributing files to devices. Use this to install applications simultaneously to multiple devices or to update files or drivers on multiple devices.
- **Monitoring:** Installs the monitoring agent on the selected device. The monitoring agent allows for many types of monitoring, including direct ASIC monitoring, in-band IPMI, out-of-band IPMI, Intel AMT, and CIM.

7. In the **Configuration** boxes, select the type. If this is dimmed, it is because you have already selected the type. It is shown for information only
8. Select a reboot option.

Rebooting manually means that devices won't reboot even if the selected agents require a reboot. You must manually reboot the device. If the device requires a reboot, installed agents won't work correctly until the device reboots. Rebooting servers if necessary reboots devices only if a selected agent requires a reboot.

Note: Only devices that update existing 8.5 agents require a reboot.

9. In the **Inventory** tab, set the Inventory Scanner configuration settings. These are explained below.

    - **Automatic update:** Remote devices read the software list from the core server during software scans. If this option is set, each device must have a drive mapped to the LDLOGON directory on the core server so they can access the software list. Changes to the software list are immediately available to devices.

- **Manual update:** The software list used to exclude titles during software scans is loaded down to each remote device. Each time the software list is changed from the console, you must manually resend it to remote devices.
- **Inventory scanner settings:** The time the inventory will run. You can select frequency, and you can specify that it always runs on startup. You can run the scanner manually from the managed server; you can launch it from **Start | Programs | LANDesk Management | Inventory Scan**. In Linux, you should be logged in as root, and run the following from the command line: /usr/LANDesk/ldms/ldiscan -ntt

  If you select the inventory scanner's **Between hours of** option, you can specify an hour range that the scanner can run between. If a device logs in during the time range you specify, the inventory scan runs automatically. If the device is already logged in, once the starting hour arrives the inventory scan starts automatically. This option is useful if you want to stagger inventory scans on devices so they don't send scans all at once.
- **Always run on startup:** The inventory scanner runs every time the device is started.

10. In the **Remote control** tab, select the type of agent to install.

    - **Service:** The agent runs as a service, and runs in the background. It uses NT-based security.
    - **On-demand:** The agent only runs when needed. It uses certificate-based security.

11. Click **Save changes** to save the agent configuration.

For more information about deploying to devices, see Understanding the device configuration architecture at the end of this chapter.

Deploying to Windows 2000/2003 servers

This product supports a scheduled, push-based configuration method, allowing you to deploy agents remotely.

To enable a push-based configuration of Windows 2000/2003 servers not already running the standard LANDesk agent, you must supply the LANDesk scheduler service with the proper login credentials as follows:

1. On the core server, click **Start | All Programs | LANDesk | LANDesk Configure Services**, then click the **Scheduler** tab.
2. Click **Change login**.
3. In the **User name** and **Password** fields, specify a domain administrator account (in the format domain\username).
4. Stop and restart the scheduler service.
5. From the Web console, target the desired devices, then click **Agent configuration > Scheduled task** to deploy the configurations.

You can specify the domain administrator when configuring Windows 2000/2003 members that belong to the same domain as the core server. To configure Windows 2000/2003 servers in other domains, you must set up trust relationships. Remember that the account identified in step 3 above is also the account under which the scheduler service will run on the core server. Make sure the account has the **Log on as a service** right.

If a push configuration fails and displays a message that says "Cannot Find Agent," try the steps listed below to identify the problem. These steps mimic the scheduler's actions during a push configuration.

1. Find the user name under which the scheduler service is running.
2. On the core server, log in with the username you found in step 1.
3. Map a drive to \\server name\C$. (This step is the one most likely to fail. It may fail for two reasons. Most likely, you don't have administrative rights to the server. If this user name doesn't have administrative rights, it's possible that the server's administrative share (C$) is disabled.)
4. Create a directory \\server name\C$\$ldtemp$ and copy a file into it.
5. Use the Windows Service Manager and try starting and stopping services on the server.

Verifying successful completion of remote control, inventory, and the standard LANDesk agent deployment

To verify that you've successfully deployed remote control, inventory, and the standard LANDesk agent to devices, confirm that you can do the following tasks from within the console. If you need additional information to complete these tasks, refer to the chapters in the *User's Guide* that correspond to the respective features.

Remote Control

- Right-click a device in the **My devices** list, then click **Remote control**. Do this for a sampling of devices.
- Perform all real-time access features: file transfer, run program, and reboot for a sampling of devices.

Inventory

- In the **My devices** list, double-click a device, then view the list of installed agents.
- Perform an inventory query.
- Select a device, then click **Inventory** to view data for that device.
- Modify a Windows device's WIN.INI file, rescan the device, then verify that changes were recorded within the CHANGES.LOG.

Deploying devices from the command line

You can control what components are installed on devices by using command-line parameters with SERVERCONFIG.EXE.

You can launch SERVERCONFIG.EXE in standalone mode. It's located in (system drive)\Program Files\LANDesk\Server Manager\LDLogon on the core server.

SERVERCONFIG.EXE can also be found in the \\coreservername\LDLogon share, which is readable from any Windows 2000/2003 server.

Deploying to Linux devices

To deploy devices in Linux, as a root user you need to complete the following steps:

1. Copy the contents of the \ldlogon\unix\linux\ directory down to the Linux machine.
2. Copy the core certificate (\ldlogon*.0) to the same directory as you copy the content in step 1. This core certificate allows the Linux machine to communicate securely with the core.
3. From the \ldlogon directory, copy the script file "Default Linux Server Configuration.sh" to the same directory used in steps 1 and 2.
4. Rename the script file to "pull.sh" or some other name without spaces, The script needs to be run in the directory you copied to, with the command $PWD/pull.sh. This script deploys the agentry to the device.

Deploying to devices using Software Distribution packages

You can use a software distribution (SWD) self-extracting package to install LANDesk agents onto devices. Devices need to have the software distribution agent on them for this feature to work.

To create an agent configuration package

1. Create an agent configuration.
2. Click **Distribution**, and create an **executable** package which includes SERVERCONFIG.EXE, including appropriate command-line parameters. See **Distribution** in the *User's Guide* for more information.

Understanding the agent configuration architecture

Configuring Windows servers

You will typically use the **Configure Agents** tab to change the settings in SERVERCONFIG.INI. This product also ships with default agent configurations. When you create an agent configuration and click the **Set as default** option, the settings are saved to the SERVERCONFIG.INI file.

Understanding SERVERCONFIG.EXE

SERVERCONFIG.EXE is LANDesk Software's device configuration utility. It configures Windows servers for management in three steps:

1. SERVERCONFIG determines whether the computer has been previously configured by another LANDesk product. If it has, SERVERCONFIG removes the older files and reverses any other changes.
2. SERVERCONFIG looks for a hidden file called CCDRIVER.TXT to decide whether the server needs to be (re)configured. (The decision process SERVERCONFIG goes through is covered below.) If the device doesn't need to be (re)configured, SERVERCONFIG exits.
3. If the device does need to be (re)configured, SERVERCONFIG loads the appropriate initialization file (SERVERCONFIG.INI) and executes the instructions contained in it.

To specify the language of the product you want to install on the device, add the line

`[serverconfig] language=`*`(three-letter language code in CAPS)`*

in SERVERCONFIG.INI, then run STAMPER.EXE to update the configurations, SERVERCONFIG will only put the specified language files on the device. You can install multiple languages by separating the language codes with a comma (for example, "FRA, DEU"). If this parameter is empty, all language files are installed on the device.

If you run SERVERCONFIG.EXE a second time and select different agents than the first execution, the agents from the first execution will be deleted. For example, if you run SERVERCONFIG.EXE and select remote control and mirror driver agents, then later decide to install SWD on top of what you installed the first time, unselecting remote control and selecting only SWD, SERVERCONFIG removes remote control and mirror driver without notifying you, and then puts down only the SWD agent. You will need to select each agent you need with each new running of SERVERCONFIG.EXE, even though you have installed the agents previously.

The following command-line parameters are available for SERVERCONFIG.EXE:

Parameter	Description
/I=	Components to include (quotation marks included): "Common Base Agent" "Inventory Scanner" "Alerting" "Remote Control" "Mirror Driver" "Vulnerability Scanner" "Software Distribution" "Server Monitor" You can combine these on the same command line. For example, Example: SERVERCONFIG.EXE /I="Mirror Driver" /I="Vulnerability Scanner"
/IP	Configure using IP
/L or /Log=	Path to the CFG_YES and CFG_NO log files that log which devices were and were not configured
/LOGON	Execute [LOGON] prefixed commands
/N or /NOUI	Do not display the user interface

/NOREBOOT	Don't reboot device when done
/NOCERT	Undo the need for digital certificate authentication, the older security method available as an option in earlier product versions.
/P	Ask for user permission to execute
/REBOOT	Force reboot after running
/TCPIP	Same as IP (see above)
/X=	Components to exclude Example: SERVERCONFIG.EXE /X=SD
/CONFIG=	/CONFIG]= Specifies a device configuration file to use in place of the default SERVERCONFIG.INI file. For example, if you've created configuration files called NTTEST.INI, then use this syntax: SERVERCONFIG.EXE /CONFIG=TEST.INI The custom .INI files should be in the same directory as SERVERCONFIG.EXE and note that the /config parameter uses the filename without the 95 prefix.
/? or /H	Display help menu

Deploying the standard LANDesk agent

The standard LANDesk agent is a required agent, and is the underlying protocol of the product.

Deploying software distribution

Software distribution automates the process of distributing files to devices. Use this agent to install applications to multiple devices or to update files or drivers on multiple devices.

Software distribution uses a Web or file server to store packages. Devices access this package server when downloading a package. You'll need to configure a package server as described in the *User's Guide*. You can deploy the software distribution agent to devices before you set up a package server.

Software distribution requires the standard LANDesk agent components.

Deploying remote control

The remote control feature enables you to view and take control of a remote device anywhere on your network. Once the remote control agents are in place, you can use any console to initiate a remote control session, where you can view, manipulate, and interact with the device as if you were logged into it locally.

You can also send files to or retrieve files from the remote device, launch applications, perform maintenance, reboot the remote device, and watch POST messages from the users console redirector.

Remote control is designed to prevent unauthorized access and to allow the level of end-user control you want.

- **Windows NT security/local template:** This security model uses a Windows NT Remote Control Operators group. Members of this group are allowed to remote control devices.
- **Certificate-based/local template:** This is the most secure option. It's also known as on-demand secure remote control.

When you select on-demand secure remote control, note the following:

- Remote consoles authenticate with the core server.
- The remote control agent on a server loads on-demand once a remote control session is authorized by the core.
- All remote control authentication and traffic is encrypted over an SSL connection.
- Once a remote control session is over, the remote control agent unloads from the device.

Remote control requires the standard LANDesk agent component.

Deploying the vulnerability scanner

The vulnerability scanner agent performs both scan and repair operations. The **Schedule security tasks** button creates a task which launches vulscan.exe with no parameters. When launched with no parameters, vulscan figures out where its core is by accessing the registry key “hklm\software\intel\landesk\LDWM”, value “CoreServer”. It then requests the latest list of vulnerability information to scan for, performs the scan, and submits the results to the core. The results are placed into the **Detected vulnerabilities** list. Detected vulnerabilities must be downloaded to the core. Vulnerabilities can be patched through the remediation process. If the remediation process successfully installs one or more patches, it will re-scan and submit new results to the core.

Deploying the remote control mirror driver

The mirror driver remote control agent lets the person remote-controlling a device view it in much deeper detail. The mirror driver can improve performance significantly by reducing the time required to detect, capture, and compress screen changes.

During the mirror driver installation, the screen on the device you are installing to goes blank briefly because the product is installing a video driver that changes the screen resolution. This is normal and does not cause any harm to the machine.

Deploying the inventory scanner

You can use the inventory scanner to add devices to the core database and to collect devices' hardware and software data. The inventory scanner runs automatically when the device is initially configured. The scanner collects hardware and software data

and enters it into the core database. After that, the hardware scan runs each time the device is booted, but the software scan only runs at an interval you specify.

Deploying the Monitoring agent

The monitoring agent allows for many types of monitoring, including direct ASIC monitoring, in-band IPMI, out-of-band IPMI, Intel AMT, and CIM.

Upgrading

Upgrading to Server Manager 8.6 can be a complex process that requires careful planning. You should already be familiar with fundamental Server Manager concepts and deployment considerations covered thoroughly in this guide, though you may want to review some of the planning overview sections. We recommend that you read this section in its entirety before performing an upgrade installation of Server Manager 8.6. Before following the steps here, make sure you back up your database.

There are two main upgrade types:

- In-place: This type of upgrade installs Server Manager 8.6 over an existing Server Manager installation.
- Side-by-side: This type of upgrade installs Server Manager 8.6 to a new core server.

There are also two main upgrade paths:

- Upgrade from Server Manager: Architecturally the 8.5 Server Manager versions are very similar. The 8.5 upgrades all use the existing database instance. Setup will upgrade your existing database to the 8.6 schema. If you specify a new database instance during the upgrade, setup won't migrate data from the old instance to the new instance.

On an in-place upgrade, CoreDataMigration.exe creates backup folders for these files. The backup subfolders appear under the folders containing these items in the new path:

- Queries are stored in the database.
- Network view groups are stored in the database.
- Agent configuration files in LDLogon.

On a side-by-side upgrade, CoreDataMigration.exe moves these files from the old core/path to the new core/path:

- Custom scripts.
- OS Deployment files.
- 8.5 custom column layout files.
- 8.5 security certificates in LDLogon and Program Files\LANDesk\Shared Files\cbaroot\certs (side-by-side upgrades only).

When doing a side-by-side upgrade, you must stop all of the LANDesk and Intel* services on the 8.5 core before you can begin installing the 8.6 core.

In order to take advantage of improved security and other enhanced features, you must redeploy the new Server Manager agents to managed devices as soon as possible after upgrading the core server and database to Server Manager 8.6. For more information on the new authentication and security model that is part of Server Manager 8.x, see the "Configuring device agents" chapter in the *User's Guide*.

If your core server has LANDesk agents on it from a previous Server Manager release, it will fail the autorun's prerequisite check. You must remove the old agents

by running uninstallwinclient.exe from the \Program Files\LANDesk\ManagementSuite folder.

Assumptions

You need to consider a number of issues before performing a Server Manager upgrade:

- All core servers and databases should be backed up or imaged prior to upgrading any LANDesk software.
- Several add-on tools and enhancements exist that can be used in conjunction with Server Manager, including some tools developed by third-party vendors. The upgrade/migration process documented in this guide does not take these tools into consideration. You should uninstall these tools before upgrading. If they're compatible with 8.6, you can reinstall them after the upgrade.
- Upgrading assumes a working knowledge of Server Manager.

Upgrading from Server Manager 8.5

In Server Manager 8.5, most data and preferences are stored in the database. Since an upgrade uses the existing database, that data is preserved.

When you run setup on a 8.5 core server, it detects that you're doing an upgrade. Setup looks for existing Server Manager products and tells you which ones it will upgrade. You won't be prompted for additional components to install. On an upgrade, setup installs the same configuration as your old version. After setup finishes, you can rerun the 8.6 setup to add or remove components.

On an upgrade, setup uses the existing security certificate from your older Server Manager version. During setup, you won't be prompted to enter information for a new certificate.

When upgrading from 8.5, 8.6 setup may apply some patches to 8.5 before doing the upgrade to 8.6. The patch application may prompt you to reboot. If it does, reboot and rerun setup, which should then begin the upgrade process normally.

To upgrade from 8.5 to 8.6

1. Back up your Management Suite database.
2. If you installed the Server Manager agents to the core server, uninstall them by using uninstallwinclient.exe. This utility is in the core server's ManagementSuite folder.
3. On your core server, install Server Manager 8.6. Check the **Do you wish to migrate your core settings...** option at the end of setup.
4. When setup finishes, activate Server Manager 8.6 (**Start | All Programs | LANDesk | Management Suite | Core Server Activation**).
5. Re-install any OSD PXE representatives.
6. Deploy the Server Manager 8.6 agents to all devices. The agent installer will automatically uninstall previous agent versions.

Migrating from a test environment to a production environment

You may want to validate Server Manager in a test environment before rolling it out company-wide. The following scenario assumes that you'll be installing to a core server in a test lab and that you'll be using a copy of your production 8.x database. Only the database will be upgraded. First, you must create your test environment.

Creating a test environment

1. Back up your existing database and restore in your test environment.
2. During the Server Manager 8.6 setup, supply the information to use your existing database. At the end of the install, Server Manager updates your database to the version 8.6 schema, preserving the data in it.
3. Run your validation tests against Server Manager 8.6.

Once you've finished validating in your test environment, you can plan the move of the test environment to your production environment. You can move your 8.6 core server from your lab environment to your main network. However, you don’t want to bring your test database to the main network because you’d end up losing all the changes that occurred during your validation phase. Instead, do the following.

Moving the test environment to your production environment

1. Once you’re ready to roll Server Manager 8.6 out company-wide, move your 8.6 core server from your lab environment to your main network.
2. Back up your production database.
3. Once the backup is complete, run SvcCfg.exe (**Tools | Configure services**). On the **General** tab, change the database connection information to point to your production database. Whenever you make a change on the **General** tab, SvcCfg.exe will make a quick check to make sure your database version is in sync with the version of your datamart.xml file. If your datamart.xml version is newer than your database version, you will be prompted to upgrade your database. Answer **Yes** and SvcCfg.exe will upgrade your database.

Uninstalling the product

Just as there's a specific strategy you should follow to deploy the different components, there's a corresponding strategy for uninstalling the components.

The following sections show you how to properly uninstall each component. You must uninstall the components in this order:

1. Uninstall LANDesk agents from devices.
2. Resetting the database.
3. Uninstall the core server.

Uninstalling LANDesk agents from devices

The first step to uninstall LANDesk software from your network is to uninstall its agents from your devices.

To uninstall agents from servers

1. Log in at the server with administrative rights.
2. Map a drive to the core server's LDMAIN share.
3. Open a command prompt, change to the LDMAIN share's drive letter, and enter the following:

   ```
   uninstallwinclient.exe
   ```

4. The uninstall will run silently, removing all agents.

You can also select **Start** > **Run** >\\core name\ldmain\uninstallwinclient.exe.

You can also send a blank agent configuration to your managed devices. See Phase 5: Creating a device setup configuration for steps, and deselect all agents. Push this configuration to the devices.

To remove the Linux agent completely from a Linux server

1. In the LDMAIN share, find the linuxuninstall.tar.gz file and copy it to the Linux box.
2. Execute this file, using the x, z, and f options. The command line should read

   ```
   tar xzf linuxuninstall.tar.gz
   ```

3. After the file is executed, run ./linuxuninstall.sh from the command line.

For help on this file, run it with the -h option.

The only file remaining after the uninstall is the /etc/ldiscnux.conf file. This file was left there to facilitate keeping the database from being cluttered with duplicate

devices. If you are not going to be putting this device back into the database, you may safely delete the file.

To push an agent:

1. Target devices in the **My devices** list.
2. In the left navigation pane, click **Agent configuration**, right-click the configuration you want to push, and click **Schedule task**.
3. In the left pane, click **Target devices**, and click the **Add target list** button.
4. Click **Schedule task**, click **Start now** to start the task immediately or **Start later** and set the task's start date and time, and click **Save**.

   You can view the status of the task in the **Configuration tasks** tab.

UninstallWinClient.exe is in the LDMain share, which is the main ManagementSuite program folder. Only administrators have access to this share. This program uninstalls Management Suite or Server Manager agents on any device it runs on. It's a Windows application that runs silently without displaying an interface. You may see two instances of the server in the database you just deleted. One of these instances would contain historical data only, while the other would contain data going forward.

Note: By default, Uninstallwinclient.exe reboots the device after uninstalling the agents. To avoid the reboot, you can add the /noreboot switch to the command line.

Running this program won't remove a device from the core database. If you redeploy agents to a device that ran this program, it will be stored in the database as a new device.

Resetting the database

To reset the database using CoreDBUtil

1. From the landesk\ManagementSuite folder on the core server, run COREDBUTIL.EXE.
2. After COREDBUTIL connects to the database, click **Reset database**, and click **OK**.

   There is no way to cancel this operation. All data in the database will be destroyed.

Uninstalling the core server

The final step in uninstalling the product from your network is to uninstall the software on the core server. Before you do so, make sure you've uninstalled the LANDesk software agents from your servers.

To uninstall the core server

1. Go to the core server.
2. Click **Start** | **Settings** | **Control Panel,** then double-click **Add/Remove Programs**.

3. To uninstall product software, select **LANDesk® Server Manager** and any other LANDesk products you installed.
4. Click **Add/Remove**.

Uninstalling the core database
You need to manually uninstall the core database. For more information, refer to your database manual.

To uninstall the remote control viewer from devices

1. Shut down all instances of your browser.
2. Click **Start** | **Settings** | **Control Panel,** then double-click **Add/Remove Programs**.
3. Click **Remote Control Viewer**, then click **Add/Remove**.
4. Click **Yes** to remove the application.
5. Click **OK** when the uninstall is completed.

Appendix A: Troubleshooting

You can reach LANDesk Software's online support services on the Web (available in English only). The services contain the most up-to-date information about LANDesk Software products. You can also find installation notes, troubleshooting tips, software updates, and customer support information. Visit the Web site below, then access the product page:

http://www.landesk.com/support/index.php

You can also download the latest versions of the Release Notes and documentation, which may include information that wasn't available at the time the product was shipped.

If you can't resolve your issue using this guide or by consulting the LANDesk Software support Web site, LANDesk Software offers a range of paid support, consulting, and partner services. For more information, see the customer support page at:

http://www.landesk.com/wheretobuy/

Before calling for customer support issues, have this information ready:

- Your name, the name of your company, and the version of the product you're using.
- The network operating system you're using (name and version).
- Any patches or service packs you've installed.
- Detailed steps to reproduce the problem.
- Steps you've already taken to troubleshoot the problem.
- Any information unique to your system that may help the Customer Support engineer understand the problem, such as what kind of database application you're using, the brand of video card you've installed, or the make and model of the computer you're using.